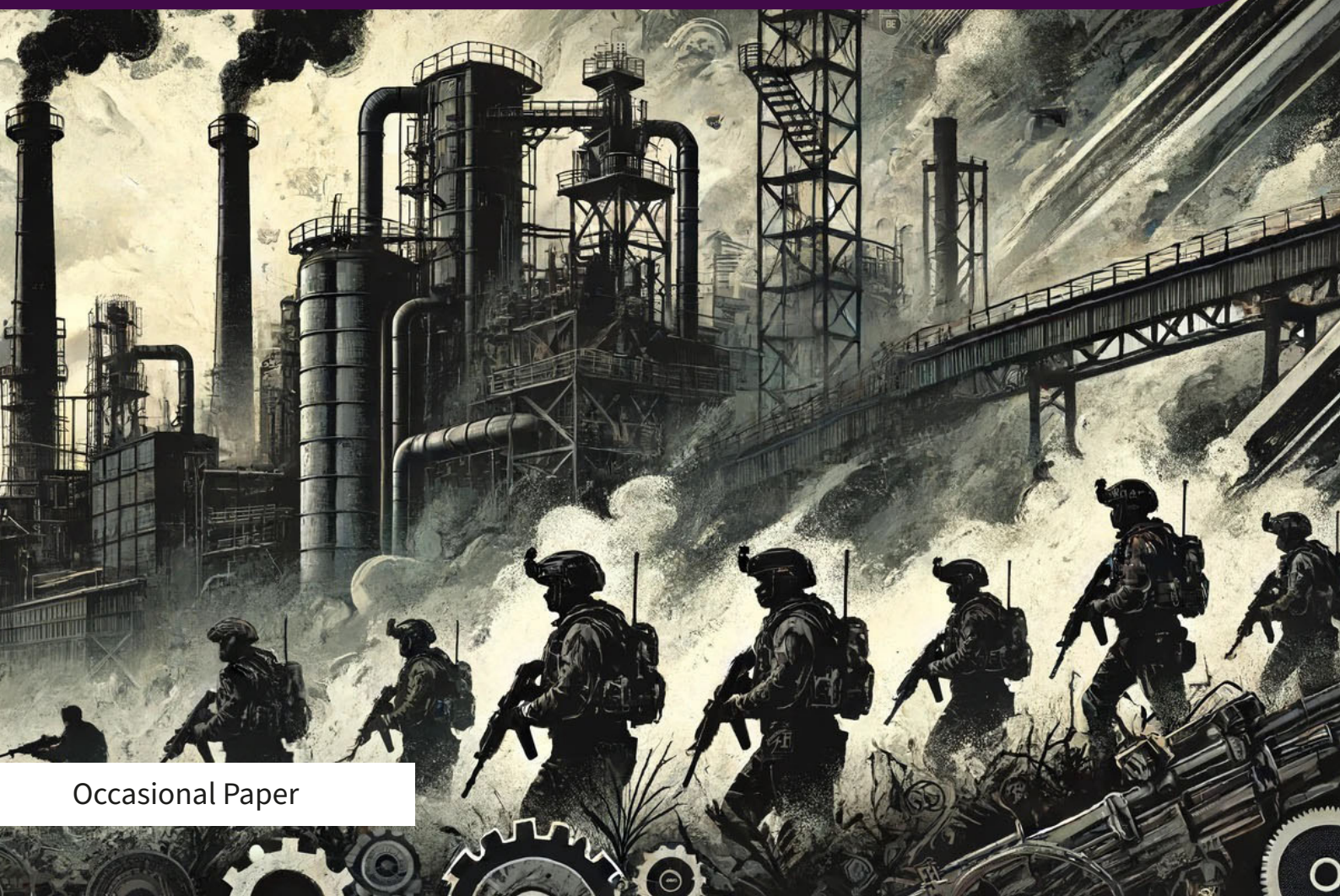
www.rusi.org

Occasional Paper

A Methodology for Degrading the Arms of the Russian Federation

Jack Watling and Gary Somerville



Occasional Paper

193 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 193 years.

Published in 2024 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2024. ISSN 2397-0286 (Online).

Cover image: Created using Chat GPT and edited by Gary Somerville

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Disclaimer

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

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

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

For this 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.

Contents

Executive Summary

Ukraine's international partners have been seeking to curtail Russian defence production through the sanctioning of Russian-affiliated individuals and entities and the disruption of Russian sanctions circumvention and covert procurement of military components on the international market since 2014. This effort accelerated after Russia's full-scale invasion of Ukraine on 24 February 2022. Despite a considerable amount of government effort, it has so far failed to have a material impact. Russia has continued to access critical components from abroad, expanded the production of core weapons, and continued to increase the sophistication of some key capabilities.

Failure to limit Russian defence production is not inevitable. Russia is highly dependent on access to raw materials, machine tooling and components for its weapons that it must source from abroad, often from NATO member states. Failure to adequately choke Russia's access to critical foreign-origin materials and components to date has arisen from three primary causes:

1. Governments have been overly reactive, rather than proactive, in disrupting Russian procurement networks. These efforts have therefore persistently been too slow.
2. Governments have tried to conduct the relevant work at too high a classification, with the ability to scale actions to disrupt Russian procurement hindered by the challenges imposed on sharing time-sensitive targeting data between multiple law enforcement entities and the private sector, on which sanctions enforcement relies.
3. Governments have also been slow to grant permission for interventions that collectively could have made a difference, because many officials and policymakers have maintained unrealistic expectations on how to measure effect. Rather than preventing Russian weapons reaching the front, efforts can degrade the reliability of systems, reduce the volume produced, or increase the price, imposing difficult trade-off decisions on Russia's military over the longer term.

Addressing these shortcomings in efforts to counter Russian military production requires the collaboration of a coalition of contributing states. These states should form an intelligence fusion centre, premised on building a common recognised target picture of the Russian defence industry, and drawing on unclassified and declassified materials. This should form the basis for identifying key bottlenecks and opportunities for disruption, communicating these opportunities to the private sector, and then synchronising and sequencing enforcement action to maximise the disruptive effect on Russian industry.

Visibility among participating official bodies of the unclassified synchronisation matrix should also enable observer countries to synchronise unilateral covert actions to expand these effects and reach parts of the Russian industrial processes that sit beyond what is reachable by overt methods. A recognised common target picture and shared synchronisation matrix should also enable deconfliction of actions between Ukraine's international partners.

The methodology guiding this effort should be to identify the key classes of Russian weapons, to identify each step in the process of supply, production and distribution, and to target it end to end, so that lags, shortages and loss of key capabilities afflict Russian defence production. The broad target categories that should be mapped and assessed include:

- **People**: procurement agents, couriers, financiers, lawyers, engineers and machinists.
- **Tooling**: machine tools, spare parts and software.
- **Components and materials**: nitrocellulose, microelectronics, metals, fibres and fuels.
- **Enablers**: revenue, ships, corporate structures, insurance mechanisms and warehousing.

Introduction

Ukraine's international partners have committed to enabling Ukraine to preserve its sovereignty in the face of sustained Russian aggression.[1] NATO has also adopted a new deterrence posture in anticipation of a major and sustained threat from Russia in the event that Moscow's campaign in Ukraine succeeds.[2] The outcome of Russia's invasion of Ukraine and the credibility of NATO's deterrence are, in the first instance, a consequence of the balance of conventional forces between NATO and Russia. Since NATO's industrial base is critical to sustaining Ukraine, it is ultimately NATO's production as compared to Russia's that underpins deterrence. One line of effort critical to succeeding in enabling either Ukraine's survival or NATO's security is to expand the defence production capacity of NATO members.[3] The other side of the net assessment, however, is the level of Russia's military–industrial production.

Russia's defence industries are far from self-sufficient. All of Russia's complex weapons are dependent on microelectronics manufactured by NATO members and other states, including South Korea, Japan, Switzerland and Taiwan.[4] A significant proportion of Russia's machine tooling is procured from companies outside Russia.[5] Access to many of the raw materials necessary for explosive energetics production and fabrication is shaped by international supply. Given that access to these components plays an important role in determining the output of Russian industry, it is in the interests of those supporting Ukraine or contributing to NATO's deterrence to explore how they can constrain, diminish or disrupt Russia's military production. The delivery of European security must in part be based on the disarmament of Russia. It is not feasible to fully disarm Russia via such means. Nevertheless, the volume of key weapons systems available can be reduced. The reliability of systems can be degraded. The robustness of Russian planning assumptions about supply can be challenged.

Noting the importance of degrading Russian military production, several countries have taken deliberate repeated steps to try to harmonise efforts to limit seepage of components made in their countries, or manufactured abroad, to Russia. This

1. UN General Assembly Resolution, 'Aggression Against Ukraine: Resolution', ES-11/1, 2 March 2022, A/RES/ES-11/1.
2. NATO, 'NATO 2022 Strategic Concept', 29 June 2022, <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf>, accessed 22 March 2024.
3. Alex Vershinin, 'The Return of Industrial Warfare', *RUSI Commentary*, 17 June 2022.
4. James Byrne et al., 'Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine', RUSI, 8 August 2022.
5. Rhodus, 'How Does Russia Make Missiles?', Rhodus Intelligence Report, no date, <https://www.rhodus.com/how-does-russia-make-missiles>, accessed 22 March 2024.

has largely revolved around the adoption of export restrictions related to Russia and a regular drumbeat of updates to sanctions lists, the interdiction and seizure of identified shipments, and the prosecution of a limited number of individuals. There has also been a systematic effort to identify and disseminate information about the breadth of Russia's dependence on access to these components, such as the publication in the UK, the US, the EU and Japan of the Common High Priority Items List.[6] As will be detailed hereafter, most of these efforts have been manifestly ineffective. There may well be covert activities carried out by states that have disrupted Russian industry, but the expansion of Russian production of war material speaks for itself to demonstrate that any such efforts have been insufficient. The volume of components reaching the Russian defence industry has consistently met the requirement, and Russia has increased the production of key platforms and systems throughout the war. There are multiple reasons for this, but at its core, the failure to transform intent into effect is a result of a lack of methodologically rigorous targeting, coordination and collaboration, both within and between governments.

Given the stakes, and the failure that has characterised these efforts to date, this paper endeavours to map what is required to have a tangible impact on Russia's defence industries. The purpose of the paper is to provide a methodology for target and effect selection and synchronisation to constrain Russian defence production. This is informed by the systemic study of Russia's weaponry, its production dependencies and access points, and the tools available to deliver effects through those action points.

The paper has three chapters. Chapter I examines the problems that have bedevilled recent attempts to curtail Russia's defence production. Chapter II takes a case study of a weapons system to map out the relevant dependencies in its production. Chapter III outlines a methodology for how those dependencies can be exploited to disrupt the production of key weapons.

This paper considers efforts to disrupt the Russian defence industry globally. Officials in various states may protest at some of the loopholes discussed, or limitations in approaches to sanctions enforcement, on the basis that they are aware of these issues and have taken steps to mitigate them. This paper is not an audit of each country's approach, but rather assesses the aggregate effectiveness of what is a global system. Thus, while some of the criticisms made in this paper may not apply to all countries mentioned in the paper, where the criticisms are applicable to the practice of some countries endeavouring to disrupt Russia's defence industries, the likelihood is that that country can be used as a route for sanctions evasion.

6. Foreign, Commonwealth & Development Office (FCDO), 'Russia Sanctions – Common High Priority Items List', updated 22 February 2024, <https://www.gov.uk/government/publications/russia-sanctions-common-high-priority-items-list/russia-sanctions-common-high-priority-items-list>, accessed 7 April 2024.

I. Why a Methodology is Needed: Assessing the Causes of Failure

The level of dependence on foreign-supplied components in the Russian defence industries was significant prior to the full-scale invasion of Ukraine. Russia's most modern tanks rolled into Ukraine equipped with French-made thermal sights, while their bodies had been cut by exquisite machine tooling manufactured across Europe, the US and Taiwan.[7] Its cruise and ballistic missiles struck Ukrainian cities guided by field-programmable gate arrays manufactured in the US. Russia's artillery hammered Ukrainian soldiers in their defensive positions with explosive payloads manufactured from German nitrocellulose, and supported by UAVs critically dependent on Dutch pressure sensors and bespoke servo motors made by a South Korean-owned factory in the Philippines.[8] Russian air defences denied Ukraine access to its skies thanks to oscillators acquired from a British company prior to the invasion, while Russian electronic warfare and signals intelligence systems used crystals supplied by Japan.[9]

Before assessing the impact of efforts by Ukraine's partners to limit ongoing access to these components and materials since the invasion, it is important to briefly outline these measures.

Immediately following Russia's full-scale invasion, the EU, the US and the UK immobilised the assets of Russia's central bank held overseas, with much ongoing discussion as to whether they can be seized.[10] Alongside these measures, many countries began a process of sanctioning Russian nationals and corporate entities associated with Russian politicians and officials. Sanctions caused assets to be frozen, and anyone doing business with these individuals or entities risked also becoming sanctioned, thus isolating the targets from the financial systems and

7. Anastasia Korotkova, 'How Russia Imports Machinery for Arms Production and Can it be Stopped', *Important Stories*, 17 April 2024, <https://istories.media/en/stories/2024/04/17/machinery-for-arms-production-imports/>, accessed 31 May 2024.
8. Author inspection of Shahed-136s in Ukraine, October 2022.
9. For a survey of these dependencies, see Byrne et al., 'Silicon Lifeline', pp. 8, 28 and 29. The crystal sets from Japan were examined by the authors in captured equipment in Ukraine in August 2022.
10. Marc Jones and Jan Strupczewski, 'Explainer: How will the West Use Russia's Frozen Assets?', *Reuters*, 21 March 2024; Paolo Tamma, Laura Dubois and Sam Fleming, 'The Clash Over Whether to Commandeer Russia's Frozen Assets', *Financial Times*, 3 May 2024.

trade that touched the economies of sanctioning states. Trade in key categories was also prohibited for certain industries, with the threat of sanctions against those facilitating such transactions as outlined in US Executive Order 14066, issued on 8 March 2022.[11] Given the significance of private businesses functioning as wallets for the Russian state,[12] a heavy emphasis was also placed on freezing the assets and holdings of Russian oligarchs.[13] After it became apparent that Russian weaponry was heavily dependent on components that were not previously subject to export controls, restrictions on the goods that could be shipped to Russia increased, as reflected by the Common High Priority Items List.[14] These sanctions regimes were initially highly patchy, but have become more comprehensive and aggressive over time. Further US Executive Orders, such as 14114, issued on 22 December 2023,[15] have endeavoured to close further avenues for financing Russian illicit procurement. Over time, sanctions packages have become more focused and comprehensive in targeting networks, reflecting a growing understanding of how the Russian defence industry functions.[16]

Initial efforts across governments were often sporadic and siloed. There was also a significant gap between the rhetorical messaging around sanctions, the actual rate at which governments were able to sanction Russian entities, and the enforcement necessary to make sanctions have a tangible effect.[17] In some countries, a capacity shortage redirected the same teams from counterterrorist finance to counter-Russia efforts. In others, it simply took time to build both cross-government teams and awareness of efforts by different departments of state. International cooperation has slowly expanded but remains messy. Enforcement has also begun to accelerate. The arrest and prosecution of individuals from the Netherlands to New York demonstrates that enforcement is happening.[18]

11. 'Prohibiting Certain Imports and New Investments with Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine', Executive Order 14066 of March 8, 2022, *Federal Register* (Vol. 87, No. 47, 10 March 2022), <https://ofac.treasury.gov/media/919031/download?inline>, accessed 7 May 2024.
12. See Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (London: William Collins, 2020).
13. Tom Keatinge, 'Combating Kleptocracy: Lessons from the Response to Russia's War in Ukraine', *RUSI Occasional Papers* (April 2024).
14. FCDO, 'Russia Sanctions – Common High Priority Items List'.
15. 'Taking Additional Steps with Respect to the Russian Federation's Harmful Activities', Executive Order 14114, 22 December 2023, *Federal Register* (Vol. 88, No. 246, 26 December 2023), <https://www.federalregister.gov/documents/2023/12/26/2023-28662/taking-additional-steps-with-respect-to-the-russian-federations-harmful-activities>, accessed 7 May 2024.
16. Daphne Psaledakis, 'US Issues Hundreds of Sanctions Targeting Russia, Takes Aim at Chinese Companies', *Reuters*, 1 May 2024.
17. Tom Keatinge and Jane Ngan, 'Walking the Talk: Threats and Ambiguity in Western Sanctions on Russia', *RUSI Commentary*, 3 February 2023.
18. *Reuters*, 'Netherlands Arrests Three for Illegal Exports to Russia', 23 January 2024; Jonathan Stempel, 'New York, Canadian Defendants Charged in the US with Exporting Technology to Russia', *Reuters*, 31 October 2023.

One challenge has been raising awareness among industry actors about how they are manipulated by Russian front companies, and how they can guard against this. Beginning in summer 2022, the US and others began significant efforts at capacity building and liaising with industry to endeavour to tackle upstream flows of goods to Russia. Further, there has undoubtedly been a significant volume of covert activity aimed at disrupting supply chains, as has been the case in almost all previous major conflicts.

And yet Russian defence production – still dependent on Western components – continues to expand.

Assessing the Extent of Failure

An assessment of Russian production demonstrates that, despite all the above measures, efforts to curtail the Russian defence industry have thus far in aggregate failed.

Russian artillery – the backbone of its battlefield successes – consumes vast quantities of ammunition. Nevertheless, at the beginning of 2022, Russian industry was producing a mere 250,000 rounds of 152 mm ammunition per year. By the beginning of 2023, it had increased production to 1 million rounds per year. Over the course of 2023, Russian production of 152 mm shells rose further, so that the country expects to manufacture 1.325 million rounds in 2024.[19] Meanwhile, 122 mm artillery ammunition increased to an expected output of 800,000 rounds over 2024.[20] The production of multiple launch rocket systems (MLRS) started from a much lower base, but has increased at a faster rate. In 2023, Russian 122 mm Grad production was just 33,000 rounds, but in 2024, production is on track to exceed 500,000 rounds. Similarly, 220 mm Uragan rocket production was just 2,800 rounds in 2023, but is on track to reach 17,000 rounds in 2024, with a similar rate of increase anticipated into 2025. This prioritisation of MLRS production is intended to compensate for shortages of replacement barrels in 2025.[21]

In addition, Russia has set about refilling and restoring the approximately 20% of its pre-war munitions stockpile that was severely degraded. Combined with munitions orders from Iran, Belarus, Syria and North Korea[22] – also heavily sanctioned – Russian overall munitions availability is likely to remain steady at

19. Russian Ministry of Defence (MoD) reports on past and projected munitions production, reviewed by the authors in February 2024.
20. *Ibid.*
21. *Ibid.*
22. James Byrne, Joseph Byrne and Gary Somerville, 'The Orient Express: North Korea's Clandestine Supply Route to Russia', RUSI, 16 October 2023; contractual agreements between the states concerned for the provision of munitions were seen by the authors in May 2023.

4 million munitions for 2024 and 2025. Despite efforts to curb this increase among Ukraine's international partners, Russia has continued to be able to import nitrocellulose from Germany, Türkiye and Taiwan, and other precursors for explosive energetics from around the world, to sustain this rapid expansion of its munitions production.[23]

A similar story can be told about Russia's manufacture of long-range missiles. One of the cruise missiles most widely employed by Russian forces during the full-scale invasion of Ukraine has been the Kh-101.[24] In 2021, prior to the full-scale invasion, the Russian Ministry of Defence (MoD) had a target of producing 350 of these missiles per year. Actual production was just 56 missiles. In 2022, the Russian MoD set a target of producing 460 Kh-101s per year. By 2023, actual production had reached 420 Kh-101s per year, not only dwarfing pre-war production, but also closing the gap between Russia's ambitions and its outputs.[25] At the beginning of 2023, Russia had approximately 50 9M723 ballistic missiles left in stock.[26] Before the full-scale invasion of Ukraine, Russia produced approximately six of these missiles per month.[27] Production has since more than tripled, such that, despite using Iskanders throughout 2023, Russia began 2024 with 180 9M723 and 9M727 in stock.[28]

Shahed-136 production, meanwhile, has similarly expanded drastically. Original Iranian production rates were close to 40 per month. Between Russia and Iran, current production of these munitions has surpassed 250 per month.[29] Given that all these munitions are critically dependent on US- and foreign-origin microelectronics, these figures clearly demonstrate that sanctions and other measures have entirely failed to slow production. Indeed, in some instances, access to specific components has increased. When the Russian military began to drop aerial bombs with UMPK glide kits, they were guided by Kometa-M satellite navigation modules using antennae from the Irish company Taoglas.[30] Despite these components being identified early in 2023, Russia has not only significantly increased production of Kometa-M, now using it across a number of UAVs including Geran-2s, but has also developed an eight-antennae array for

23. Trade data shows significant flows of nitrocellulose from these states to Russia over the course of the year. Trade data supplied by third-party commercial provider.
24. Ian Williams, *Putin's Missile War: Russia's Strike Campaign in Ukraine* (Washington, DC and Lanham, MD: Center for Strategic and International Studies and Rowman & Littlefield), 2023, p. 27, <https://www.csis.org/analysis/putins-missile-war>, accessed 22 February 2024.
25. Reports to the Russian MoD on missile production during 2023, seen by the authors in February 2024.
26. Assessment of the Ukrainian intelligence community, briefed to the authors in Ukraine in February 2024.
27. *Ibid*.
28. Reports to the Russian MoD on missile production during 2023, seen by the authors in February 2024.
29. Assessment of the Ukrainian intelligence community, briefed to the authors in Ukraine in February 2024.
30. Sean Pollock, 'Parts Made by Irish Tech Company Allegedly Found in 500 Kg Russian Bomb in Ukraine', *Irish Independent*, 16 July 2023.

the UMPK, doubling the number of Taoglas antennae used per system.[31] The Russian MoD assesses that the impact of Western sanctions on production of key weapons systems has been to impose a 30% increase in the price of microelectronic components.[32] This is not trivial, but it is also manageable.

The picture of Russian armoured vehicle production is distorted by the volume of equipment that the Russians can withdraw from storage and refurbish. For example, Russia is producing approximately 1,500 tanks and 3,000 other armoured fighting vehicles in 2024 and is set to produce a similar number in 2025.[33] Approximately 85% of these are vehicles refurbished from storage. Nevertheless, the number of newly produced vehicles has also been rising. For example, the Kurganmashzavod plant produced 100 BMP-3 infantry fighting vehicles during Q1 2023. In Q2, this rose to 108 vehicles. In Q3, 120 BMP-3s rolled off the production line and in Q4, 135 were produced.[34] This increase may seem modest, but it shows that Russia is steadily expanding production capacity. In some cases, this is achieved by cutting corners and reprioritising. For example, in 2023, Russia produced 728 Tigr-M, a rate that is anticipated to fall to 721 in 2024, while the level of environmental protection from chemical, biological, radiological and nuclear threats on the vehicle is being reduced. This frees up capacity elsewhere. There is also some substitution away from components sourced from the US and Europe. Refurbished tanks, for example, had used Catherine thermal sights made by Thales before the full-scale invasion of Ukraine.[35] Refurbished tanks today are instead fitted with Chinese- or Belarusian-supplied tank sights, which are less capable, but adequate.[36] Here, therefore, there has been some successful import substitution. Ultimately, however, the refocusing on capability requires changes to machine tools, and large volumes of these continue to flow to Russia from the US, Europe, Taiwan and further afield, along with the software updates to run them.

In summary, despite the diligent efforts of many civil servants, backed by the political will to disrupt Russia's military–industrial output, there is little to show for it. The question arises as to why efforts so far have proven so ineffective. This may in part be answered with reference to the initially chaotic approach to building the sanctions architecture, with the presumption that it will become more effective over time. However, this paper argues that there are also long-

31. Author inspection of UMPK and multiple Kometa-M modules across several Russian platforms, Ukraine, February and April 2024.
32. Report from the Russian defence industry to the Russian MoD concerning challenges in meeting production targets, seen by the authors in February 2024.
33. Reports to the Russian MoD on armoured vehicle production during 2023, seen by the authors in February 2024.
34. Production figures from the Kurganmashzavod plant, seen by the authors in February 2024.
35. Author inspection of captured Russian vehicles, Ukraine, June 2022.
36. Recently captured Russian vehicles, Ukraine, February 2024.

term, systemic challenges in how governments are approaching the issue. The remainder of this chapter suggests that there are three structural problems in how governments approach the issue:

1. Being reactive rather than proactive.
2. Over-classifying information and thus not fully empowering the private sector charged with implementing sanctions.
3. Having unrealistic expectations of success that warp targeting.

Understanding these causes of failure is critical if an effective methodology is to be applied.

Reactive Rather Than Proactive

Following the start of the full-scale Russian invasion, there was a scramble in Western capitals to sanction Russian entities. After the initial sanctioning of big names and low-hanging fruit, a more deliberate search for Russians who actually mattered for the war effort commenced. This led, in April 2022, to the sanctioning of Vladimir Yevtushenkov, who owned Sistema, a large Russian corporation involved in a wide range of defence-related enterprises, including the production of radar, long-range missile complexes and UAVs.[37]

Despite the rapid sanctioning of Yevtushenkov and his Russian holdings, Sistema continued to function and to do significant volumes of business within Europe to sustain its work for the Russian MoD. It did this through a range of front companies. In Switzerland, Serbian national Ivan Kokeza founded ERSO Energy Solutions AG, an apparent affiliate of Yevtushenkov's ERSO Holding JSC, likely to provide funds for Yevtushenkov's structure outside the sanctions net.[38] In 2021, ERSO Energy Solutions and Kokeza were listed as shareholders in Electrozavod Group, alongside several Sistema subsidiaries.[39] Meanwhile, Waldemar Reuswich, a German with a history of engaging in controversial Russian-linked business schemes, began a round of company registrations across Europe, including taking over control of entities previously linked to Sistema, such as Segezha Packaging in Denmark.[40] At the same time, Reuswich's Swiss

37. Office of Financial Sanctions Implementation, HM Treasury, 'Financial Sanctions Notice: Russia', 13 April 2023, <https://assets.publishing.service.gov.uk/media/64381eee22ef3b000c66f1ab/Notice_Russia_130423.pdf>, accessed 29 March 2024.
38. Switzerland Registry of Commerce, document dated 18 November 2022 from Sayari Analytics, <https://sayari.com/>, accessed 31 May 2024.
39. Акционерное общество «Производственный комплекс ХК ЭЛЕКТРОЗАВОД» [Joint Stock Company "Industrial Complex HC ELEKTROZAVOD"], «Часть I. Титульный лист списка аффилированных лиц акционерного общества» ['Part I. Title Page of the List of Affiliated Persons of the Joint-Stock Company]', 14 January 2022.
40. Matthew P, 'Controversial Waldemar Reuswich Took Over Vladimir Evtushenkov's Segezha Assets', *Talk Finance,* 16 June 2023, <https://www.talk-finance.co.uk/economics/controversial-waldemar-reuswich-

Precision Holding AG[41] was also listed as a shareholder in Electrozavod.[42] Similar holding companies and fronts appear to have been established in Luxembourg and Ireland.[43] Yevtushenkov meanwhile transferred shares in Sistema to his son Felix,[44] while his daughter continued to run a firm in the UK until she was sanctioned in April 2023.[45]

The details of these structures for avoiding sanctions and enabling Sistema to continue to obtain critical components and raw materials were presented to the British authorities in early 2023. As one of the officials who received the information put it, 'we were very grateful. We looked into these people, and it turned out they were a thoroughly rotten set'.[46] Actions were taken, and some of Sistema's more ambitious schemes were disrupted. The irony of this was that while British officials were pleased with their success, so were the Russians. Russia had succeeded in continuing to obtain what it needed for almost a year after the invasion. The network of front companies was discovered, but this simply caused Russia to move on to the next scheme. In fact, Russian planning documents drawn up weeks after the invasion of Ukraine highlight how post-facto sanctions were anticipated and not seen as a setback. For the Russians, failure meant the breaking up of a scheme before materiel got through, not its discovery after it entered Russia.[47]

At the heart of the failure to prevent Sistema's circumvention of sanctions was, and is, that many official bodies targeting these entities have entirely the wrong mindset about how to use the tools at their disposal and in whose hands those tools should be placed. While the US has a long history of using sanctions against state adversaries such as Iran,[48] many European states have neither had the capacity nor the inclination to approach sanctions from the point of view of economic warfare, instead treating them as regulatory instruments or as measures

took-over-vladimir-evtushenkovs-segezha-assets/>, accessed 29 March 2024.

41. Switzerland Registry of Commerce, document dated 8 March 2024 from Sayari Analytics, <https://sayari.com/>, accessed 31 May 2024.
42. Акционерное общество «Производственный комплекс ХК ЭЛЕКТРОЗАВОД» [Joint Stock Company "Industrial Complex HC ELEKTROZAVOD"], «Часть I. Титульный лист списка аффилированных лиц акционерного общества» ['Part I. Title Page of the List of Affiliated Persons of the Joint-Stock Company]'.
43. Sayari Analytics, <https://sayari.com/>, accessed 31 May 2024.
44. Interfax, 'Vladimir Yevtushenkov Reduces Stake in Sistema to Below Controlling Amid UK Personal Sanctions', 13 April 2022, <https://interfax.com/newsroom/top-stories/78197/>, accessed 31 May 2024.
45. UK Companies House, 'Redline Capital (UK) Limited: People', <https://find-and-update.company-information.service.gov.uk/company/08971917/officers>, accessed 31 May 2024; FCDO, 'UK Sanctions Abramovich and Usmanov's Financial Fixers in Crackdown on Oligarch Enablers', press release, 12 April 2023, <https://www.gov.uk/government/news/uk-sanctions-abramovich-and-usmanovs-financial-fixers-in-crackdown-on-oligarch-enablers>, accessed 31 May 2024.
46. Conversation with the author, London, April 2023.
47. Materials seen by the author, April 2022.
48. Suzanne Maloney, 'Disarming Iran: A Story of Cybersabotage and Sanctions', *New York Times*, 28 September 2016.

to limit proliferation to terrorist groups.[49] Where there were dedicated teams both designing and implementing sanctions in Europe, most were focused on counterterrorism. Where nation states were targeted, there was more interest in the political message sent by sanctions than in their practical effect. Even in the US, where the architecture for economic warfare exists, permissions to act were less forthcoming, and mechanisms for planning sanctions and enforcement with allies and partners were limited.

Unlike terrorists, Russia can function at scale. It is notable how unsuccessful comparable attempts have been to tackle sanctions evasion by Iran, a much less capable actor than Russia.[50] It is therefore essential that those crafting and enforcing sanctions and export controls do not see the imposition of these mechanisms as the end of the process, but rather the beginning. Imposing these restrictions simply creates the legal basis to move against entities and the people facilitating the activity, but the adversary will immediately begin to shift to using alternative structures. Enforcers must, therefore, proactively use intelligence to anticipate what the new structures will be, target them pre-emptively when they are being used to conspire to violate export controls and sanctions (rather than when they have already successfully done so), and arrest those running these front companies at a pace that genuinely slows the speed of Russia's reaction. Rather than being a reactive tool, enforced when Russia succeeds in illegally importing Western components, sanctions must be used as a weapon to proactively hunt those who assist Russia, and to neutralise them before they succeed in exporting technologies. Those in the private sector in allied countries that manufacture and export these components must also be proactively engaged to understand the extent to which their components are being procured by the Russian war machine. Most importantly, this needs to be done across Ukraine's partners, rather than in siloes within each state.

A proactive approach is entirely possible to implement. The Yevtushenkov network used obvious individuals with links to his companies before the full-scale invasion to evade the effect of sanctions. The individuals involved could have been identified before even Yevtushenkov was sanctioned. But this would have required someone to ask the question. The information existed in the import, export and company registration information of the states that eventually moved against Yevtushenkov's network. But this information was not exploited because of a lack of official curiosity to retrieve it. Until the machinery of

49. Evidence given by Tom Keatinge to the House of Commons Treasury Committee, April 2024. House of Commons Treasury Committee, 'Oral Evidence: Are the UK's Russian Financial Sanctions Working?', HC 604, 30 April 2024, <https://committees.parliament.uk/oralevidence/14720/pdf/>, accessed 14 May 2024.
50. Henry Thompson and Jack Watling, 'Assessing Dynamics of Control Through Iranian Technology Transfer to Yemen's Houthis', *RUSI Journal* (Vol. 167, Issue 4–5, November 2022), pp. 64–77.

government begins to think offensively and proactively, Russia will continue to be one step ahead.

Over-Classification

Support for Ukraine has been heavily dependent on those who hold stockpiles of Soviet-legacy equipment, from fighter jets to air defence systems. Many of these countries are NATO members. Greece operates S-300 and Tor.[51] Finland operated Buk.[52] Other pieces of Russian equipment were obtained by Ukraine's international partners in Syria and Libya, such as when the US seized a Pantsir-1 air defence system.[53] Ukraine's international partners had to maintain these systems, and were therefore aware that they contained a significant number of non-Russian components. Ukraine has been pointing out the dependence on foreign-origin components in Orlan-10 since 2018. The extent of Russian dependence on Western components was therefore not a revelation to Ukraine's international partners when Ukraine began publishing images of foreign-origin chips in Russian weapons systems in April 2022.[54] It was, however, news to Western ministers, who quickly started demanding something be done about it. The curious thing is that, despite the issue being understood in detail by Western defence establishments for decades, no plan was immediately available to exploit this vulnerability in Russia's defence industries at the beginning of the war. Despite knowledge of the extent of dependence sitting in government, and there being viable means to explain how that knowledge was obtained without exposing sources and methods, it was not briefed and exploited.

The structure of classification within many governments – while critical to a range of functions – is a major problem in scaling action against Russia's military–industrial complex. During the War on Terror, two trends in intelligence contributed to the emergence of this problem. First, the need to find terrorists among a large civilian population drove investment in powerful analytical tools. The tendency towards 'need to know' that had created many lateral compartments in the intelligence community gave way to 'need to share', and the development of all-source intelligence fusion.[55] The result is that, within most governments, the experts able to analyse large data sets and the tools they need to do their job

51. James Hackett (ed.), *The Military Balance: The Annual Assessment of Global Military Capabilities and Defence Economics 2023* (London: International Institute for Strategic Studies, 2023).
52. *Ibid.*
53. Joseph Trevithick, 'The United States Smuggled a Russian-Made Pantsir Air Defense System out of Libya: Report', *The Warzone*, updated 27 January 2021, <https://www.twz.com/38964/the-united-states-smuggled-a-russian-made-pantsir-air-defense-system-out-of-libya-report>, accessed 29 March 2024.
54. Indeed, using Western components was explicit Soviet strategy during the Cold War, see Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* (London: Simon & Schuster, 2023).
55. Roger Z George and James B Bruce (eds), *Analyzing Intelligence: National Security Practitioners' Perspectives*, Second edition (Washington, DC: Georgetown University Press, 2014).

are hosted on Above Secret systems. During the War on Terror, most action was either undertaken by the military directly, or was small in scale. Thus, the intelligence community could either provide target packs (information sufficient for the planning and execution of an action) to the military, or specific declassification could be undertaken for law enforcement.

The problem when tackling an adversary like Russia is that enforcement action, if it is to have a measurable impact on production, must be executed at scale and across multiple jurisdictions, to include the private sector producers of critical components. Most of this action must be undertaken by law enforcement, and, to have the permissions to act, law enforcement must have evidence. In reality, most of the underlying intelligence necessary to build target packs aimed at the Russian defence industry is low-grade information. Most of the evidence necessary to obtain warrants for law enforcement is available in unclassified business records. The scale at which Russia operates means that much of its activity cannot be concealed except insofar as it can disappear into the noise of the general volume of business transactions. Much of it is commercially available and does not rely on covert collection.

Nevertheless, because the analytical tools sit on Above Secret systems, the data is ingested into these systems for analysis. Any product subsequently created using the data in combination with limited volumes of Above Secret-origin information receives an Above Secret classification. The release of Above Secret information to foreign law enforcement with sufficient explanation of sourcing to stand up in court as the basis for a warrant – for example – is a painstaking task. Declassification requires a review of exactly what is being declassified, what risk this poses to sources and methods, and how the information is subsequently attributed.[56] This is necessary because of the ease with which the release of Above Secret information could pose a threat to life for sources or undermine ongoing intelligence collection by revealing the capabilities of national technical means. What it also means, however, is that target packs cannot be declassified at scale.

There is a wider ongoing revolution in intelligence that offers a way round this problem. Open source intelligence allows for the harnessing of publicly accessible data to build an unclassified, robust evidence base for target packs. This can be shared freely between governments. Pioneers such as investigative journalism group Bellingcat have demonstrated how commercial systems can be used to reconstruct what would previously have only been available through national technical means.[57] This is recognised by the intelligence community. As General

56. William R Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (Washington, DC: Georgetown University Press, 2009), pp. 130–34.
57. Eliot Higgins, *We are Bellingcat: An Intelligence Agency for the People* (London: Bloomsbury, 2021).

Jim Hockenhull observed when head of UK Defence Intelligence, the majority of collection could now be of open source information, with closed sources filling the gaps.[58] This process of reconstructing evidence outside secure environments is being used by governments, but few have the capacity of expertise to do this at scale both inside and outside secure environments. This has had detrimental effects on efforts to disrupt Russia's defence industry.

For example, Russia's procurement of Nvidia microelectronics for use in image processing on its military UAVs was carried out by an individual named Igor Ievlev. It is a matter of public record that Ievlev is a graduate of the Cherepovets Military Institute of Radioelectronics, where he specialised as an engineer in radio communications.[59] Now named the Military University of Radio Electronics,[60] the institute is reportedly a training establishment for officers of the GRU (Russian military intelligence),[61] including those who specialise in the procurement of critical technologies for weapons and military equipment.[62] Ievlev made purchases from Nvidia partners who sold their chips to him directly.[63] Although Ievlev's history was known to Western governments, this information was not public, so companies had no ability to screen their millions of customers for those that might raise concerns. The result was that, despite information being publicly available, a likely GRU officer could directly procure sensitive Western microelectronics and ship them to Russia to directly support its arms industry. Western officials could subsequently use the trade data to show that a crime had been committed and close the channel. But getting ahead of the problem at the scale necessary to have an effect requires analysis to be conducted at a lower level of classification and for information to be made as accessible as possible.

58. Jim Hockenhull, 'How Open-Source Intelligence has Shaped the Russia-Ukraine War', speech at RUSI webinar, 7 November 2022, <https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war>, accessed 7 May 2024.
59. Rocket Reach, 'Igor Ievlev Email', <https://rocketreach.co/igor-ievlev-email_37309767>, accessed 29 March 2024.
60. Военный Университет Радиоэлектроники [Military University of Radio Electronics], «История» ['History'], archived 17 June 2023, <https://web.archive.org/web/20230617174158/https://vure.mil.ru/About/Istoriya>, accessed 31 May 2024.
61. Sergey Kanev, 'Rooftop Spooks: How GRU and SVR Monitor Moldovan Authorities Using Russian Embassy Rooftop Antennas', *The Insider*, 24 July 2023, <https://theins.ru/en/politics/263675>, accessed 29 March 2024; Cyber Security Intelligence, 'What is the GRU & Who Does it Hack?', 22 November 2018, <https://www.cybersecurityintelligence.com/blog/what-is-the-gru-and-who-does-it-hack-3904.html>, accessed 31 May 2024; Robert Lansing Institute for Global Threats and Democracies Studies, 'Russian Intelligence in the Netherlands: Purpose, Targets, and Scale of Penetration', 18 October 2022, <https://lansinginstitute.org/2022/10/18/russian-intelligence-in-the-netherlands-purpose-targets-and-scale-of-penetration>, accessed 31 May 2024.
62. Guildhall, «В ЦОР раскрыли российский ВУЗ, готовящий промышленных шпионов для ГРУ» ['In the COR, a Russian University that Trains Industrial Spies for the GRU was Revealed'], 17 October 2023, <https://ghall.com.ua/2023/10/17/v-tsor-raskryli-rossijskij-vuz-gotovyashhij-promyshlennyh-shpionov-dlya-gru/>, accessed 29 March 2024.
63. Trade data supplied by third-party commercial provider.

This not only facilitates coordination of law enforcement across jurisdictions, but also means that companies cannot plead ignorance when they sell to Russian front companies. This shifts the burden of proof, and thus the legal risk, creating a deterrent effect.

Unrealistic Expectations

The third major government structure problem is the way in which many of Ukraine's international partners have sought to impact Russia's defence industry, which has largely driven a cycle of inflated expectations, followed by a sense of futility when those expectations are not realised.[64] Many official concepts in the years preceding Russia's full-scale invasion of Ukraine tried to push the idea of smart power over hard power: the precise use of capabilities in order to have disproportionate effects. In the UK, this has undoubtedly been driven by diminishing capacity to operate at scale. In the US, it has arguably been driven by the threat of stretch, as challengers emerge in three separate theatres. The desire to be clever shaped a response to the Russian defence industry that emphasised which specific components would have the greatest impact if they were denied. While in and of itself an interesting question, this framing demonstrated a misunderstanding of the problem. The desire was to go after components that would prevent Russia from building key systems.

Not all components are equal, and some were more susceptible to disruption and more important for the capabilities being targeted.[65] Generally, however, there is no exhaust port on the Russian death star. The loss of a critical component will tend to lead to the alteration of the production sequence until a new supply of the component can be found, or it is substituted with an inferior component. This will impose cost and delays, and often impact the reliability of the system when it enters Russian service. But it does not stop the system being made. Two interesting examples highlight this trend.

When Shahed-136 UAVs began to hit Ukraine, it was noted that they had servo motors that manipulated their control surfaces which were built in the Philippines by South Korean-owned company HiTec.[66] Pressure was subsequently put on HiTec to stop manufacturing the product. But this did not stop the Russians and Iranians from building Shahed-136s. Ukrainian observers noted that the original

64. Inflated expectations of the impact of sanctions have been a policy problem for more than a century. See Nicholas Mulder, *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War* (New Haven, CT: Yale University Press, 2022).
65. For Egypt's missile programme, for example, it was navigation systems that were a particular challenge, see CIA Directorate of Intelligence, 'Egypt: Aspirations for Missile Production: An Intelligence Assessment', NESA 88-10024, April 1988, p. 18, <https://www.cia.gov/readingroom/docs/CIA-RDP89S01450R000200210001-2.pdf>, accessed 29 March 2024.
66. Author examination of these servo motors in Shahed-136 UAVs, Ukraine, October 2022.

servo motors were swapped for Chinese ones, and that these were of inferior quality, causing some Shahed-136s to crash and limiting the acuteness of manoeuvres the aircraft could perform, simplifying its interception by air defence.[67] As a result, Russia must launch more Shahed-136s to deliver the same effect, and has less assurance that it will be achieved.

Another good example is how Russia has responded to limitations in accessing sufficient quantities of explosive energetics. Many factories continued to fulfil orders but filled shells with less hexogen (Russian military-grade explosive). Others provided rounds with fewer charges.[68] Eventually, Russia began to import nitrocellulose with a lower level of enrichment, thus reducing the explosive energy of the charges with which it would eventually fill its ammunition.[69]

The impact at the front was therefore counterintuitive. The Russians had to fire more rounds to achieve the same level of effect or had to use higher-echelon capabilities to conduct counterbattery fire because the lower echelon systems lacked the range. Thus, the immediate effect was to increase the volume and calibre of Russian fires. The impact on consumption and therefore endurance of the Russian artillery was significant until the problem could be resolved. If the cost of producing key systems can be raised sufficiently, it will not prevent Russia from making munitions. But it will reduce how long Russia can sustain the war.

There are very few historical examples where economic efforts have decisively prevented the manufacture of a capability. The Third Reich was exceptionally effective at finding alternatives as its industries were destroyed or disrupted by blockade and bombing.[70] However, the attritional effect of measures targeting defence industries, whether in terms of cost, opportunity cost, or reliability and performance, is significant. Another important point is that any intervention will be time limited in its effect. However, sequences of disruptions can leave a system functioning in an extremely inefficient manner. The cumulative effect of restructuring can be more significant than the direct effect of a given intervention.

The reason why properly assessing the impact of interventions is important is that unless the right metrics are briefed, interventions are unlikely to achieve approval from policymakers. If policymakers expect to be given options to bring production of a Russian system to a standstill and none of the options provided

67. Author examination of a range of Shahed-136s and discussions with Ukrainian technical teams, Ukraine, February and April 2024.
68. Author examination of Russian shells, warheads and payloads carried out in Ukraine during the war.
69. Author examination of hexogen mixes over time in various Russian munitions during the war, and author examination of records of purchases from Russian defence enterprises, often recorded as supporting 'fireworks' production.
70. Adam Tooze, *The Wages of Destruction: The Making and Breaking of the Nazi Economy* (London: Penguin, 2007).

meet that threshold, it may be that none of them will receive the green light. No single operation is likely to justify itself in terms of the risks and resources involved versus the impact. However, a package of interventions over time can have a disproportionately disruptive impact. Setting the right policy expectations is, therefore, critical if permissions are to be forthcoming at a scale that has impact.

II. The Vulnerability of Russia's Supply Chains

Given the level of effort expended in sanctioning entities connected with Russia as compared with the limited effects achieved, there are some who argue that it is a fruitless endeavour. This argument can be countered when examining the Russian military–industrial enterprise and the extent of the threat surface against which Ukraine and its international partners can operate. This chapter seeks to demonstrate the level of vulnerability by offering a detailed case study of a Russian defence enterprise and its vulnerabilities.

The case study is the Zala Aero Group,[71] a now-sanctioned Russian UAV manufacturer partially owned by Kalashnikov Concern, a subsidiary of the Rostec Group defence conglomerate.[72] Zala Aero Group's and its subsidiaries' supply chains span the US, Europe and East Asia. Documents and trade data show that Zala Aero Group leans on dozens of Russian companies to procure foreign items to manufacture UAVs.

Zala Aero Group's Significance

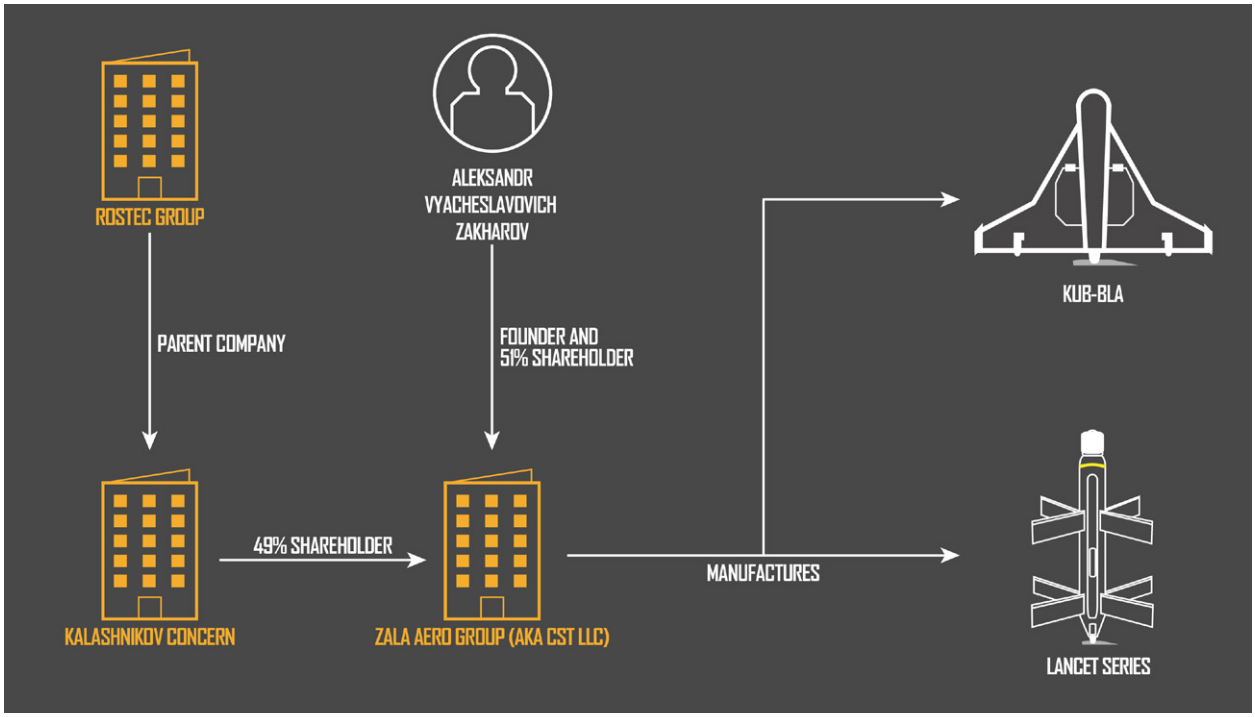
The war in Ukraine has seen an unprecedented increase in the use of UAVs as integral pieces of the reconnaissance-fires complex. One-way attack drones are increasingly used to facilitate rapid strikes against targets. The sophistication of these drones ranges from off-the-shelf first person-view models rigged with explosives to purpose-built loitering munitions with increasingly advanced sensor suites. Zala Aero Group is one of the leading companies in Russia that can design and produce UAVs and loitering munitions, offering an all-in-one reconnaissance-strike package.[73]

Zala's Lancet-3 is one of Russia's most effective loitering munitions, responsible for disabling or destroying hundreds of Ukrainian weapons platforms since

71. Technically, the company is named CST LLC (tax identification number ООО ‹ЦСТ›; INN: 1841015504), but it is more commonly named Zala Aero Group in English. See Russian Federal Tax Register, Sayari Analytics, <https://sayari.com/>, accessed 15 March 2024.
72. Roman Romanovskiy, 'Who, How and Where Buys Components for the Deadliest Suicide Drones in the Russian Army', *Important Stories*, 13 June 2023, <https://istories.media/en/stories/2023/06/13/zala-lancet/>, accessed 15 March 2024.
73. Zala Aero Group Беспилотные Системы [Zala Aero Group Unmanned Systems], «Беспилотные летательные аппараты ZALA» ['Zala Unmanned Aerial Vehicles'], archived 5 April 2023, <https://web.archive.org/web/20230405000224/https://zala.aero/>, accessed 19 March 2024.

mid-2022.[74] As a result, Russia's defence industry has placed significant emphasis on expanding production. In May 2023, Zala Aero Group's corporate owner announced the creation of a 'Division of Special Machines' to expand the output of these systems, stating that the company expects to increase production of UAVs several-fold in 2024.[75] In parallel, Russia's Ministry of Industry and Trade has drafted a strategy for the coordinated development of UAVs until 2035.[76]

Figure 1: Zala Aero Group's Ownership Structure and Sample Products



Source: Author generated with reference to Zala Aero Group, <https://web.archive.org/web/20230405000224/https://zala.aero/> and Sayari Analytics, <https://sayari.com/>.

74. Центр анализа мировой торговли оружием [Center for Analysis of the World Arms Trade], «Российская армия начала применять на Украине барражирующие боеприпасы «Ланцет» с усиленной БЧ» ['The Russian Army Began to Use "Lancet" Loitering Ammunition with Enhanced Warheads in Ukraine'], 21 July 2022, <https://armstrade.org/includes/periodics/news/2022/0721/070568601/detail.shtml>, accessed 19 March 2024.
75. Калашников [Kalashnikov], ««Калашников» открывает новое производство БЛА» ['"Kalashnikov" Opens a New Production of UAVs'], 26 May 2023, <https://webcache.googleusercontent.com/search?q=cache:5H5BnbPs0oEJ:https://kalashnikovgroup.ru/news/kalashnikov-_otkryvaet_novoe_proizvodstvo_bla&cd=12&hl=en&ct=clnk&gl=uk>, accessed 19 March 2024.
76. *Ведомости*, ««Калашников» сообщил о запуске нового производства беспилотников» ['Kalashikov Announced the Launch of a New Production of Drones'], 26 May 2023, <https://www.vedomosti.ru/technology/news/2023/05/26/977034-kalashnikov-zapuske-proizvodstva-bespilotnikov>, accessed 19 March 2024.

Zala Aero Group has begun ramping up UAV production, including of Lancet-3s, by purchasing shopping malls and converting them into manufacturing plants.[77] In February 2024, one such plant caught fire.[78]

The company's aspirations also include the development of more advanced loitering munitions that use AI to create lethal autonomous weapon systems.[79] Such an expansion will require Zala Aero Group to tap into international supply chains to acquire the requisite technology to build and field these systems.

Zala Aero Group's Procurement Networks

From January 2022 to May 2023, Zala Aero Group paid dozens of Russian companies millions of roubles for various 'products'.[80] Many of these companies are vendors, distributors and importers of the components and tools required to produce UAVs. Often, these companies' websites advertise such items – including those produced abroad.

Trade data confirms that these companies import large quantities of foreign goods, including those manufactured by Western companies.[81] Sanctions following Russia's 2022 invasion of Ukraine do not appear to have hindered these companies' ability to import dual-use, export-controlled items which, in some cases, have seen an increase in imports since February 2022.[82]

The largest recipient of Zala Aero Group's payments was Aeroscan LLC, which uses UAVs for geospatial surveying and topographical mapping.[83] Aeroscan's owner, Nikita Zakharov, is the son of Zala Aero Group's founder and majority shareholder,[84] Aleksandr Zakharov, and has appeared at several public events

77. *7x7,* 'Drones Attack a Bathhouse', blog post, 5 March 2023, <https://semnasem.org/articles/2023/03/05/drones-attack-a-bathhouse>, accessed 19 March 2024; Molfar, 'How Russians Manufacture "Shaheds" and "Lancets" in Shopping Malls: Exposing the Family of the Chief Constructor', <https://molfar.com/en/blog/rosiyany-vyroblyayut-shahedy-ta-lancety-v-trc-deanon-golovnogo-konstruktora>, accessed 31 May 2024.
78. Dinara Khalilova, 'Alleged Drone Factory Catches Fire in Russia's Izhevsk', *Kyiv Independent*, 17 February 2024, <https://kyivindependent.com/alleged-drone-factory-catches-fire-in-russias-izhevsk/>, accessed 19 March 2024.
79. Alexander Rogatkin, «Выпуск «Ланцетов» вырос в 50 раз: как работают легендарные дроны» ['The Production of "Lancets" has Increased 50 Times: How the Legendary Drones Work'], *Вести*, 16 July 2023, <https://www.vesti.ru/article/3455254>, accessed 19 March 2024.
80. Documents seen by RUSI.
81. Trade data supplied by third-party commercial provider.
82. *Ibid*.
83. Aeroscan, «О компании» ['About the Company'], <https://scan.aero/o-kompanii.html>, accessed 19 March 2024.
84. Osintflow, 'The Family of the Chief Designer of the Lancet and Orlan Uavs, Director of Zala Aero Group – Oleksandr Zakharov', 3 November 2023, <https://osintflow.com/en/news/2023-11-03/>, accessed 31 May 2024.

with the Zala Aero Group, even helping to purchase a shopping centre that was later converted into a UAV factory.[85] Aeroscan has Russian government contracts to conduct maintenance on Zala Aero Group's UAVs for government departments.[86]

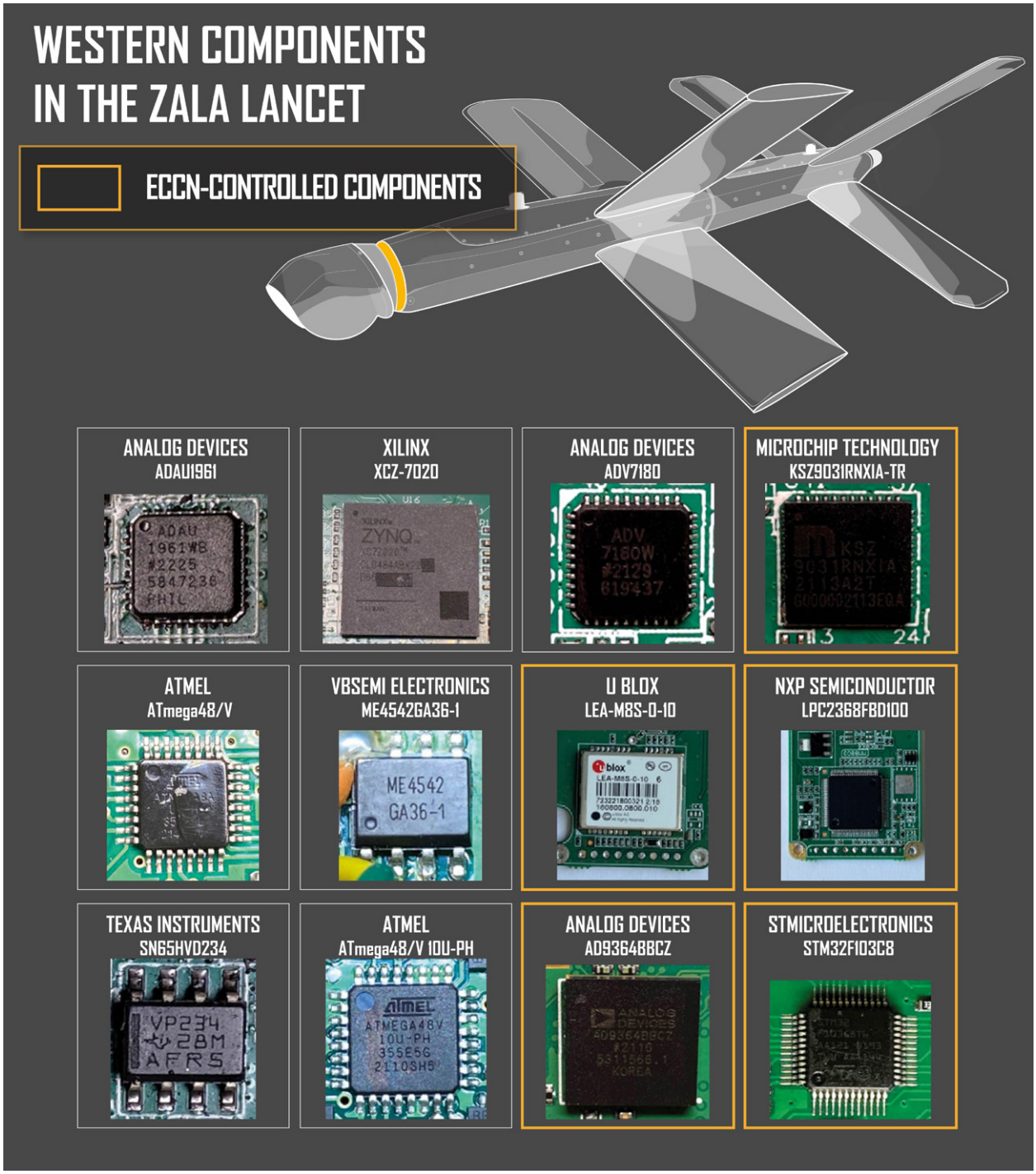
Aeroscan remitted more than RUB 2.3 billion to Zala Aero Group from January 2022 to May 2023, and Zala Aero Group remitted more than RUB 2.5 billion to Aeroscan.[87] Like Zala Aero Group, Aeroscan has not imported any items used to produce UAVs, except for a single $8,000 shipment of gas analysers in January 2022.[88] However, Aeroscan did make payments from January 2022 to May 2023 to Russian companies that import and distribute items for UAV production.[89] Zala Aero Group also paid several of the same companies that import these goods.[90] Aeroscan appears, therefore, to be procuring dual-use components and technologies for Zala Aero Group. Zala Aero Group's suppliers' trade data shows they have procured large amounts of materials and tools used to assemble UAVs.[91]

Microelectronics

Zala Aero Group's UAVs contain dozens of microelectronics: the KUB-BLA contains at least 11 components, and the Lancet-3 at least 27.[92] Almost all the microelectronics were designed by semiconductor companies in the US and Europe.[93] At least three in the KUB-BLA and five in the Lancet-3 are dual use and subject to export controls.[94]

85. *7x7,* 'Drones Attack a Bathhouse'.
86. ClearSpending, «Supplier: Общество С Ограниченной Ответственностью «Аэроскан»» ['Supplier: Limited Liability Company "Aeroscan"'], <https://clearspending.ru/supplier/inn=5603045794&kpp=771501001>, accessed 2 July 2023.
87. Documents seen by RUSI.
88. Trade data supplied by third-party commercial provider.
89. Documents seen by RUSI.
90. *Ibid.*
91. Trade data supplied by third-party commercial provider.
92. Documents seen by RUSI.
93. *Ibid.*
94. *Ibid.*

Figure 2: Western-Made Components Inside the Zala Lancet-3



Source: Author generated using documents and photographs seen by RUSI. ECCN = Export Control Classification Number.

From January 2022 to May 2023, Zala Aero Group and Aeroscan paid millions of roubles to Russian microelectronics importers,[95] many of which are now sanctioned by the US[96] and the EU.[97]

Some UAVs contain export-controlled Nvidia microchips in an apparent attempt to improve their sensor suites and, in the case of the Lancet-3, create an autonomous weapons system immune to jamming.[98] One specific Moscow-based microelectronics importer, ID Solution, is likely to be the key supplier of these Nvidia modules to Zala Aero Group and responsible for more than 90% of the Nvidia imports into Russia since the invasion began.[99] From March 2022 to December 2023, ID Solution imported more than $14 million in microchips and related items to Russia.[100]

Cameras

ID Solution also imported thousands of cameras, including ones compatible with Nvidia modules, and high-spec electro-optical cameras produced by Sony Corporation and South Korea's Wonwoo Engineering.[101] Zala Aero Group and Aeroscan also paid other Russian companies that import cameras and specialise in digital surveillance systems.[102] One of these companies received nearly RUB 200 million from January 2022 to May 2023.[103]

Batteries

UAVs require a constant supply of lithium-ion batteries, particularly for loitering munitions, when such batteries are unretrievable.[104] One company that has likely supplied Zala Aero Group with lithium-ion batteries has partnership agreements

95. *Ibid.*
96. US Department of the Treasury, Office of Foreign Assets Control, 'Russia-Related Designations, Updates and Removal; Counter Terrorism Designation Update; Issuance of Russia-related General Licenses', 2 November 2023, <https://ofac.treasury.gov/recent-actions/20231102>, accessed 19 March 2024.
97. Council of the European Union, 'Council Regulation (EU) 2024/745 of 23 February 2024 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine', *Official Journal of the European Union*, 23 February 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400745>, accessed 19 March 2024.
98. Aleksandr Khrolenko, «СВО: российские «Ланцеты» становятся умнее» ['NWO: Russian "Lancets" are Getting Smarter'], *Sputnik*, 12 February 2024, archived on 19 March 2024, <https://web.archive.org/web/20240319163249/https://ru.sputnik.kz/20240212/svo-rossiyskie-lantsety-stanovyatsya-umnee-42243765.html>, accessed 19 March 2024.
99. Documents seen by RUSI; trade data supplied by third-party commercial provider.
100. Trade data supplied by third-party commercial provider.
101. *Ibid.*
102. Documents seen by RUSI.
103. *Ibid.*
104. Documents seen by RUSI.

with more than 25 electronic component and battery manufacturers. Before the war, this company's annual imports were valued at only a few thousand dollars.[105] In 2023, however, the company imported more than $730,000 in lithium-ion batteries from Chinese companies.[106] While some batteries were labelled as produced by Chinese brands, their model numbers revealed that they were produced by Samsung.[107]

Motors

UAVs require various motors to operate. Lightweight UAVs and loitering munitions use AC motors with air blades to generate propulsion and lift. Servo motors manipulate control surfaces for balance and direction of travel, and stepper motors can stabilise and rotate gimbal-mounted cameras.

Several of Zala Aero Group's and Aeroscan's Russian customers import these types of motors, despite not appearing to specialise in supplying these products.[108] One such company was paid more than RUB 1.4 billion by Zala Aero Group[109] and has imported millions of dollars in AC motors from Chinese companies.[110] Another company also imported thousands of stepper motors from Chinese companies from March to December 2023.[111]

While intended for radio-controlled aircraft models, servo motors are also crucial components used in UAVs, and have been found in UAVs used by the Armed Forces of the Russian Federation (AFRF).[112] One Russian company imported 3,400 servo motors from HiTec RCD Philippines in December 2021.[113] Between October 2023 and December 2023, ID Solution also imported at least 400 HiTec RCD servo motors.[114] HiTec RCD servo motors have been found in the Shahed-136/Geran-2 loitering munitions used by the AFRF in Ukraine,[115] as well as in loitering munitions built and fielded by Houthi rebels in 2019.[116]

105. Trade data supplied by third-party commercial provider.
106. *Ibid.*
107. *Ibid.*
108. Trade data supplied by third-party commercial provider.
109. *Ibid.*
110. *Ibid.*
111. *Ibid.*
112. Documents seen by RUSI.
113. *Ibid.*
114. *Ibid.*
115. Documents seen by RUSI.
116. UN Security Council, 'Final Report of the Panel of Experts on Yemen', S/2020/70, 27 January 2020, p. 95, <https://www.securitycouncilreport.org/un-documents/document/s-2020-70.php>, accessed 19 March 2024.

Carbon Fibres and Polymers

High-performance UAVs, such as those produced by Zala Aero Group, often use carbon fibre and similar composite materials, as these allow UAVs to be more agile, lightweight and durable.[117]

From March 2022 to December 2023, one likely supplier of such composite materials to Zala Aero Group imported $5.6 million in acrylic polymers, epoxy resins, fibreglass fabrics and liquid polyesters.[118] The supplier's largest composite materials supplier is an Estonian company that exported synthetic materials with defence and aerospace applications produced by European companies,[119] meaning that European materials are likely to be in a range of Russian UAVs.

Machine Tools and Injection Moulding Machines

Manufacturers such as Zala Aero Group also require sophisticated machine tools and robot arms to produce UAVs. Russian state media, while visiting one of Zala Aero Group's converted shopping centre factories, showed various foreign machine tools used to manufacture Lancet-3s.[120] These were manufactured by Hyundai, DN Solutions and Fanuc Machines.[121] Additionally, Zala Aero Group uses plastic injection moulding machines purchased from Japan to synthesise components it can no longer import, including propeller blades.[122]

Zala Aero Group and Aeroscan have paid several Russian importers and distributors of machine tools and injection moulding machines,[123] one of which claims to supply industrial equipment to several sanctioned Russian defence conglomerates.[124] This distributor has historically imported machine tools from various European manufacturers.[125] Another Russian company imported more

117. Mohamed M ElFaham, Ayman M Mostafa and G M Nasr, 'Unmanned Aerial Vehicle (UAV) Manufacturing Materials: Synthesis, Spectroscopic Characterization and Dynamic Mechanical Analysis (DMA)', *Journal of Molecular Structure* (Vol. 1,201, No. 3, October 2019).
118. Trade data supplied by third-party commercial provider.
119. *Ibid*.
120. Rogatkin, «Выпуск «Ланцетов» вырос в 50 раз» ['The Production of "Lancets" has Increased 50 Times']; DrGuideTech, 'What CNC Machines are Used for the Lancet UAV Manufacturing?', *YouTube*, 22 August 2023, <https://www.youtube.com/watch?v=zdteByIJL9w>, accessed 19 March 2024.
121. Rogatkin, «Выпуск «Ланцетов» вырос в 50 раз» ['The Production of "Lancets" has Increased 50 Times'].
122. A recovered intact KUB-BLA seen by the authors had a propeller blade produced by German company Aeronaut. In an interview with Russian state media, Aleksandr Zakharov stated that, due to sanctions, he was no longer able to purchase these from the EU, and so purchased two JADS 60U injection moulding machines from Japan Steel Works so Zala Aero Group could produce their own. See Rogatkin, «Выпуск «Ланцетов» вырос в 50 раз» ['The Production of "Lancets" has Increased 50 Times']; DrGuideTech, 'What CNC Machines are Used for the LANCET UAV Manufacturing?'.
123. Documents seen by RUSI.
124. Windeq Technical Center, 'About Us', <https://en.windeq.ru/company/>, accessed 19 March 2024.
125. Trade data supplied by third-party commercial provider.

than $22.2 million in machine tools and spare parts from March 2022 to December 2023, primarily from one Hong Kong company.[126] The types of machine tools imported include those used by Zala Aero Group.[127]

Meanwhile, a third Russian company that received more than RUB 24 million from Aeroscan imported more than $4.2 million in injection moulding machines and related parts from March 2022 to December 2023.[128] These shipments included $3 million in injection moulding machines and spare parts produced by Japan Steel Works,[129] the same brand as that used by Zala Aero Group.[130]

Triaging Points of Vulnerability

Despite Russia's efforts to reduce its dependence on foreign materials for its war machine, its scramble to increase production following its invasion of Ukraine shows that it is still highly reliant on international supply chains. While sanctions and the will of companies to cut business ties with Russia impacted the country's imports in the first few months of the war, procurement networks have adapted significantly. Trade patterns show that shipments to Russia are now routed through third countries that are friendlier to Russia, are more permissive of dubious trade flows, or have porous export controls.

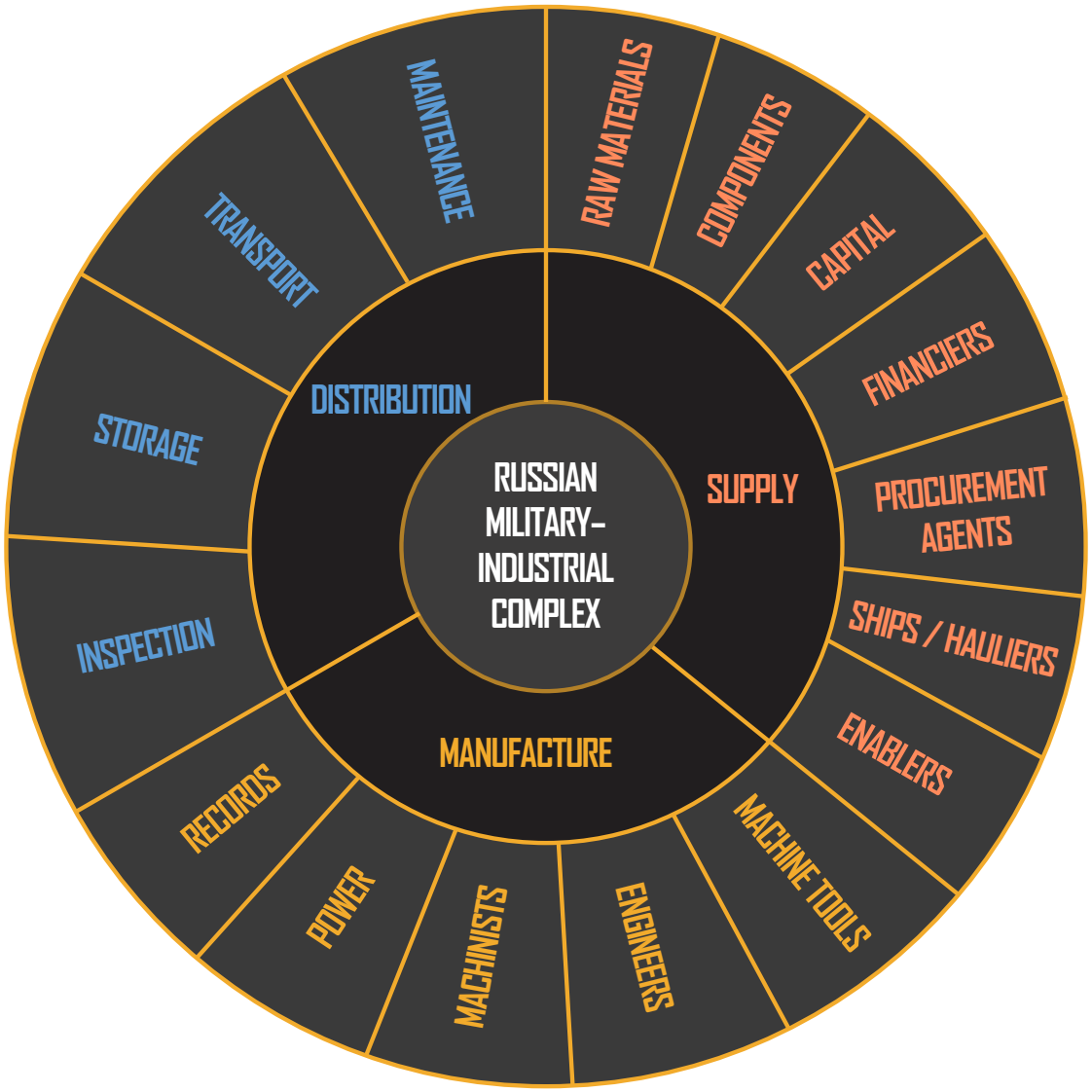
Zala Aero Group's procurement flows underscore why Ukraine and its allies must change tactics in relation to disrupting Russia's defence supply chains, by targeting the flows of specific items or technologies, instead of focusing sanctions action on the most obvious entities and individuals facilitating these networks. When targeting individuals and entities, it would be more impactful to prioritise those actors facilitating the procurement of these specific materials.

Russia's procurement of more advanced materials requires individuals outside of Russia to facilitate this procurement. For example, several owners and shareholders of Russian microelectronics importers are graduates and affiliates of military radioelectronic institutes, and many would appear to have extensive academic knowledge of microelectronics.[131] The proactive detection, investigation and prosecution of these individuals and those who assist them are critical to disrupting Russia's defence supply chains, which usually start within the jurisdiction of states with an interest in limiting Russian military–industrial output. This is especially relevant for individuals procuring European-made materials exported

126. *Ibid.*
127. *Ibid.*
128. *Ibid.*
129. Trade data supplied by third-party commercial provider.
130. Rogatkin, «Выпуск «Ланцетов» вырос в 50 раз» ['The Production of "Lancets" has Increased 50 Times'].
131. Rocket Reach, 'Igor Ievlev Email'. Note that this was a major line of effort for Directorate T of the First Chief Directorate of the KGB, since taken over by the SVR. See Miller, *Chip War*, pp. 141–44.

directly from the EU to Russia, as Western allies have greater purview in these jurisdictions.

Figure 3: Russian Military–Industrial Complex Sequential Target Categories



Source: Author generated.

Companies such as Zala Aero Group require a constant supply of specific components and materials to sustain UAV production, and these same materials are used across all Russian military-grade UAVs. Stemming the flow of these components would have more significant ramifications for Zala Aero Group's production cycle than targeting the company and its leadership alone. Procurement networks, instead of merely having to reorganise through unsanctioned companies connected to unsanctioned individuals, would also have to source completely new materials, at great expense in terms of funding, time and resources.

Targeting the supply of industrial equipment like machine tools, milling machines, lathes and injection moulding machines is equally imperative. Russian defence manufacturers rely on and will continue to need additional industrial equipment – along with regular maintenance and access to spare parts – to expand production. Although Russia has gradually imported larger quantities of Chinese machine tools,[132] it also continues to source these tools from companies in the US, Europe, Japan, South Korea and Taiwan.[133]

Targeting this supply would force these networks to prioritise analogous components and tools of lower quality, or unreliable counterfeits, increasing the chance of failure and degrading the overall effectiveness of Russian systems in Ukraine. The integration of new components and tools is also an arduous, time- and labour-intensive process, as replacements are tested and certified for battlefield use. This is particularly important as Zala Aero Group seeks to improve its UAVs with more advanced technologies – including AI capabilities – which would be difficult to replace adequately.

132. Joe Leahy et al., 'China's Advanced Machine Tool Exports to Russia Soar after Ukraine Invasion', *Financial Times*, 2 January 2024.
133. Trade data supplied by third-party commercial provider.

III. A Methodology of Effects

The previous chapters have outlined the extent to which existing approaches to disrupting Russia's defence industry have failed. In Chapter I the causes of failure were identified as: a reactive approach taken by governments; over-classification resulting in siloed and exclusive actions taken at too small a scale; and unrealistic expectations of what can be achieved. Chapter II demonstrated that the effort to disrupt Russia's defence industries is far from futile, given the large threat surface against which Ukraine's international partners can operate. This chapter therefore proposes an approach to targeting and synchronisation of actions to deliver relevant effects at scale.

Building a Recognised Common Target Picture

Fundamental to scaling the disruption of Russia's defence industry is ensuring that the various bodies involved – intelligence, customs, law enforcement, sanctions units, financial institutions, industry and militaries – have a detailed understanding of the target and how it is functioning. Moreover, this picture must be accessible to the relevant bodies, in multiple countries, with as little latency as possible. The effective interdiction of a shipment may well require that a purchase traced from Country A is flagged to law enforcement in Country B before it is exported to Country C, and that a warrant is issued and relevant action taken immediately. The foundational requirement for such a rapid process to succeed is for states to have a shared picture of Russia's industrial system, and to agree that this picture is sufficient to form the basis for planning actions.

The framework for building a recognised common target picture (RCTP) of Russia's defence industry should be a confidential but unclassified data fusion centre hosted by one state as a framework nation, and with liaison officers from a coalition of willing states. Which country acts as the framework nation is clearly a matter for negotiation. The core of this fusion centre should be a network map of Russian procurement channels and manufacturing systems, databases of associated corporate entities and individuals, and financial flows. The fusion centre must have the full range of commercially available analytical tools, and participating states should enable access to import and export data, transaction

records, company records and other relevant databases from participating countries. Using investigative powers, states should also request trace data from financial institutions and make it available to the fusion centre. In some cases, ingesting these data sets may be periodic or may be subject to access requests. This should therefore be managed by participating analysts from contributing countries. Each country is also likely to have a significant volume of commercial trade data and company records obtained through technical collection. While individual records from these sets may be sensitive insofar as they reveal points of access, in aggregate, these data sets are often very low-level intelligence because they have so many potential points of origin. To that end, analysts from participating states with security clearances should be able to assess what their countries hold at Secret and Above Secret classifications away from the fusion centre and, understanding the gaps in the fused picture, be able to request the declassification and sharing of key data sets. In many cases, this may simply be the sharing of prompts taken from collection – names of individuals or specific companies – that can be flagged to the analysts at the fusion centre to target when trawling publicly available information.

Perhaps one of the most important effects that can be delivered by the team managing the RCTP is the ability to publish an approved subscriber database that key industry partners can log in to to screen their customers and get greater insight into their downstream supply chains. The existence of such a database could remove the legal protection of pleading ignorance, shifting the legal jeopardy onto suppliers and thereby creating a deterrent effect against turning a blind eye to profitable orders for products to dubious clients.

If one group of analysts is focused on maintaining an accurate picture of where Russia is procuring material, where it is going, what it is being used for, and who is involved in obtaining it, two additional teams are also necessary. The first is a team responsible for assessing opportunities to disrupt. The basis for this should be to analyse dependency within the system and to evaluate the resilience of the system to interference at each stage. The result is comparable with a road map showing congestion, which must also indicate where intervention can have the greatest effect. The broad target categories that should be mapped and assessed include:

- **People**: procurement agents, couriers, financiers, lawyers, engineers and machinists.
- **Tooling**: machine tools, spare parts and software.
- **Components and materials**: nitrocellulose, microelectronics, metals, fibres and fuels.
- **Enablers**: revenue, ships, corporate structures, insurance mechanisms and warehousing.

The third team of analysts should be tasked with producing target packs, mainly on request by participating countries, to package parts of the RCTP to be presented to courts, policymakers and others to authorise interventions or to release the target pack to non-participating countries for the purpose of diplomacy. This team needs to understand the legal frameworks of participating states, so that fused data can be turned into actionable information. Another function of this team should be to allow participating states to observe the activities being prepared by others. A challenge that has confronted Ukraine's international partners so far has been deconfliction. With activities at higher classification or in compartments, and without mechanisms for deconfliction, shipments that one state allowed to pass in order to gather data on who would redirect it have been stopped by a different state. Multiple states have also wasted time and energy trying to act against the same shipment. By having a multinational team building these packs, it becomes possible for deconfliction issues to be flagged and addressed.

The significance of the framework nation is that it should control the security cell and access to the fusion centre. The work of the fusion cell should be based on confidentiality – as is the case with law enforcement – rather than classification. To that end, the framework nation should be able to exclude analysts if they breach confidentiality. The sensitive element of the fusion centre's work is its relationship with planned actions, rather than the RCTP itself. There is a precedent for such an approach. The counter-piracy command-and-control centres in Singapore and the Bab al-Mandab, for example, necessarily involved participating states which needed a common operating picture to deconflict their activities, but which were also competitors.[134]

It could be argued that such a structure will be too easily penetrated by Russia. To a large extent, as long as there is latency in Russia's access to certain materials, this will not disrupt enforcement and is not overly problematic. It is also clear that these problems are manageable. The support effort for Ukraine, coordinating the delivery of material from a large number of countries, is a good example of how operations can remain sufficiently secure to enable the mission while being largely unclassified but with specific elements of the effort managed at higher classification. Many of the countries supporting Ukraine are not Five Eyes states, or even NATO members, and Ukraine itself is acknowledged to be a penetrated bureaucracy that must have sight of shipments. In spite of this, Russia has so far failed to interdict shipments. The security issues are real, but they can be managed.

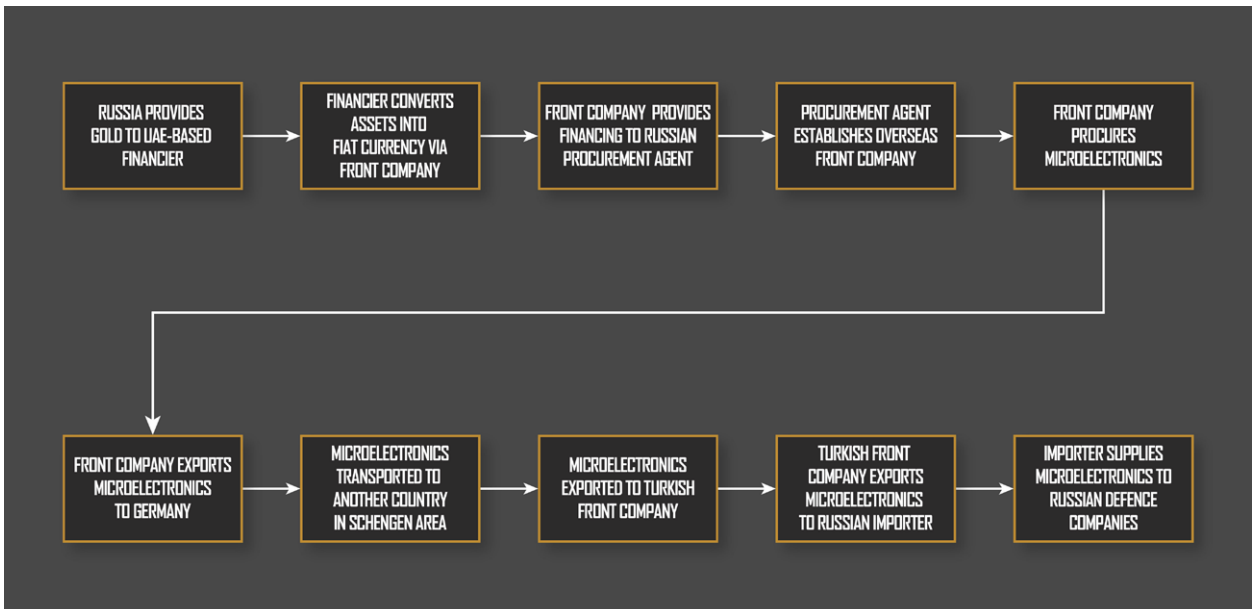
134. Bruce D Jones, *To Rule the Waves: How Control of the World's Oceans Shapes the Fate of the Superpowers* (New York, NY: Simon & Schuster, 2021), pp. 167–78.

Synchronising and Layering Effects

While states will hold information at higher classification that will be withheld from an RCTP, the most sensitive element of the work of the fusion centre is planning interventions to impact Russia's defence industry. The identification of key target sets by the fusion centre should form the basis for minilateral or unilateral effects planning, with the level of classification appropriate to the participants involved. Nevertheless, if effects are going to scale, then most will be unclassified and implemented by various branches of the participating states' official bodies.

If a targeting board were convened to assess options against an identified procurement network, it would become possible for participating states to propose actions to disrupt the procurement that collectively leave very few reversionary options for Russia. Synchronising effects thereby allows amplification of impact. Where there are gaps in interventions that different countries have proposed, this can become the area of focus for unilateral measures planned at higher classification.

Figure 4: A Typical Russian Procurement Network

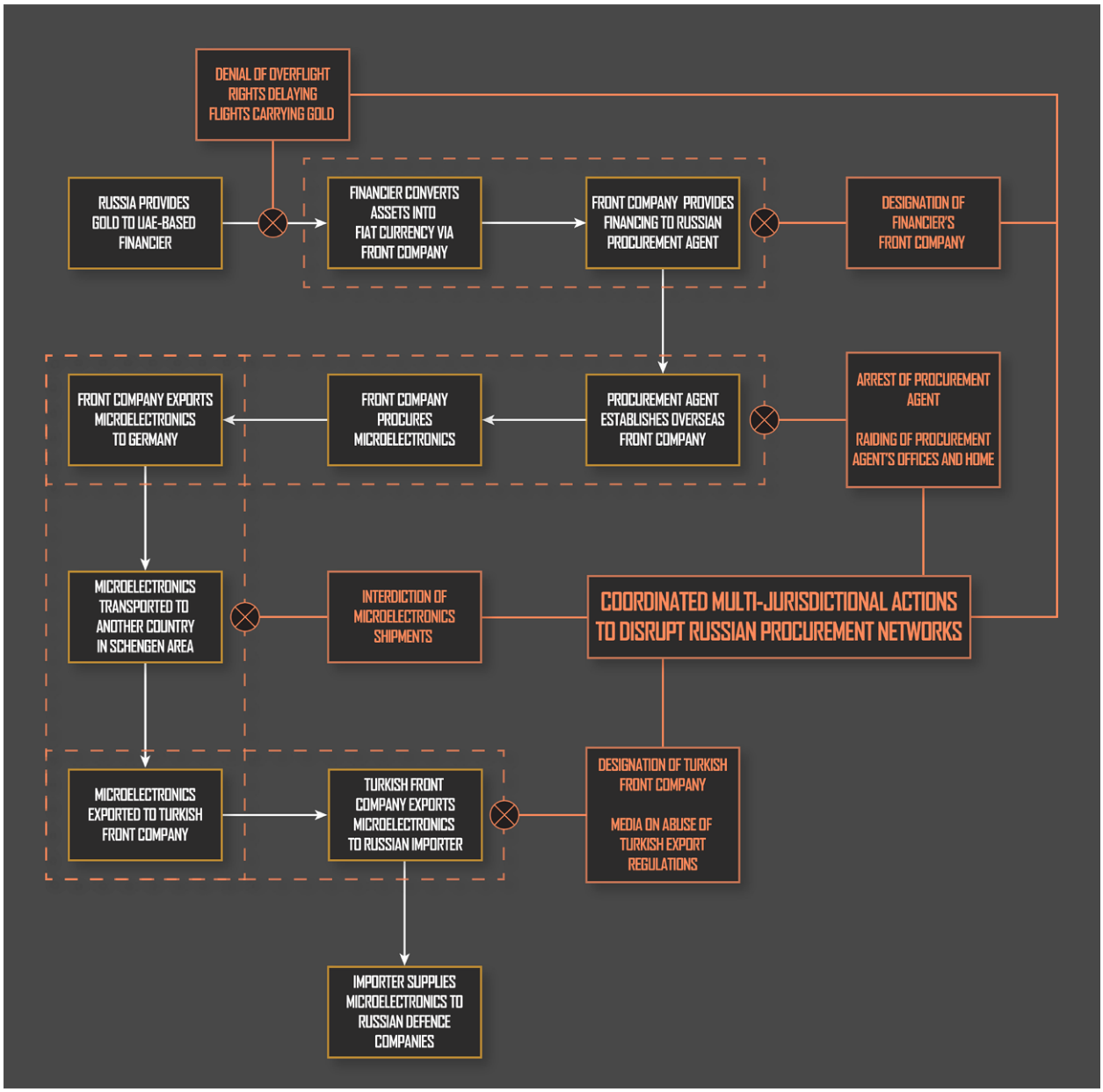


Source: Author generated.

For example, consider the following procurement scheme. A Russian dual national is financed to purchase US microelectronics via a front company and ship them to Germany, where they will be driven to another country in the Schengen Area, exported to another front company in Türkiye, and then be mislabelled and shipped to Russia. The finance for the operation might be provided by a Russian gold shipment converted to cash in the UAE under the

auspices of a front company and thereafter made available to the procurement agent. A single action – such as interdicting the shipment – might disrupt it, but if the procurement agent is not detained and is warned off by the seizure, they can simply restart the process using an alternative front company. If sanctions are applied against the importing company in Türkiye, a different one can simply be used.

Figure 5: How Coordinated Multi-Jurisdictional Actions Can Disrupt a Russian Procurement Scheme Across Multiple Points



Source: Author generated.

However, if the sanctioning of the Turkish company, the raiding of the procurement officer's home, and the media publication of the abuse of Turkish customs

regulation can be synchronised, it is difficult for an alternative route to be set up quickly. If, at the same time, the flight carrying the gold can be denied overflight rights and so delayed, and the company converting the gold to capital sanctioned simultaneously, the funds may not be available to pursue an alternative avenue of supply. This of course requires collaboration between several countries. It also becomes possible for other states to be in a position to add friction to Russia's activities as required. This could mean getting Russian actors excluded from a flight, for example, so that they are stuck in a jurisdiction where they can be detained while the other actions are taken. If we imagine, therefore, a synchronisation chart showing the steps for the Russian procurement and manufacture of a system along one axis, and the measures being lined up by the participating states to simultaneously disrupt each stage, then the cost to Russia will be high. Procurement agents and other enablers are less replaceable than front companies. And, of course, pooling evidence gathered during seizures to the fusion centre to refine the RCTP allows for the cycle to be accelerated and the impact of each intervention magnified.

It is necessary to consider the impact of not only actions taken in parallel, but also those taken in sequence. The prevention of a large shipment reaching a Russian factory may have a fairly limited impact on production. The factory may use stockpiled components to get itself over the stop in supply while alternative procurement channels are established. Alternatively, the stockpile may be used to allow engineers to work out a substitute Chinese component – albeit potentially reducing reliability – so that output can continue even if the part does not become available. However, suppose the disruption of a supply route is staggered with the subsequent disruption of the financing of supply routes, and that the actions against the alternative supply route are worked out in advance. Suppose then that once the engineers have become satisfied with a substitute component, there is disruption to the functioning of their machine tooling. While they are resolving the issue with the tooling, production is disrupted so that supplies of other materials begin to accumulate in storage at the factory. But as they are close to resolving the supply issue, the Ukrainian military uses one-way attack UAVs to destroy or damage a significant quantity of the stockpiled material. This kind of sequencing, such that production remains continuously off balance, inefficient and disrupted, is likely to have a far wider impact on output – both quantitative and qualitative – than any single action.

The scale of effect that is needed against Russia's defence industry, and the lead roles of both law enforcement in taking enforcement action, and private sector manufacturers and exporters in ensuring integrity in their supply chains, mean that the bulk of activities must be conducted in the confidential but unclassified space. There are discrete actions, however, reaching targets beyond legal jurisdiction, that some participating countries may wish to pursue using covert

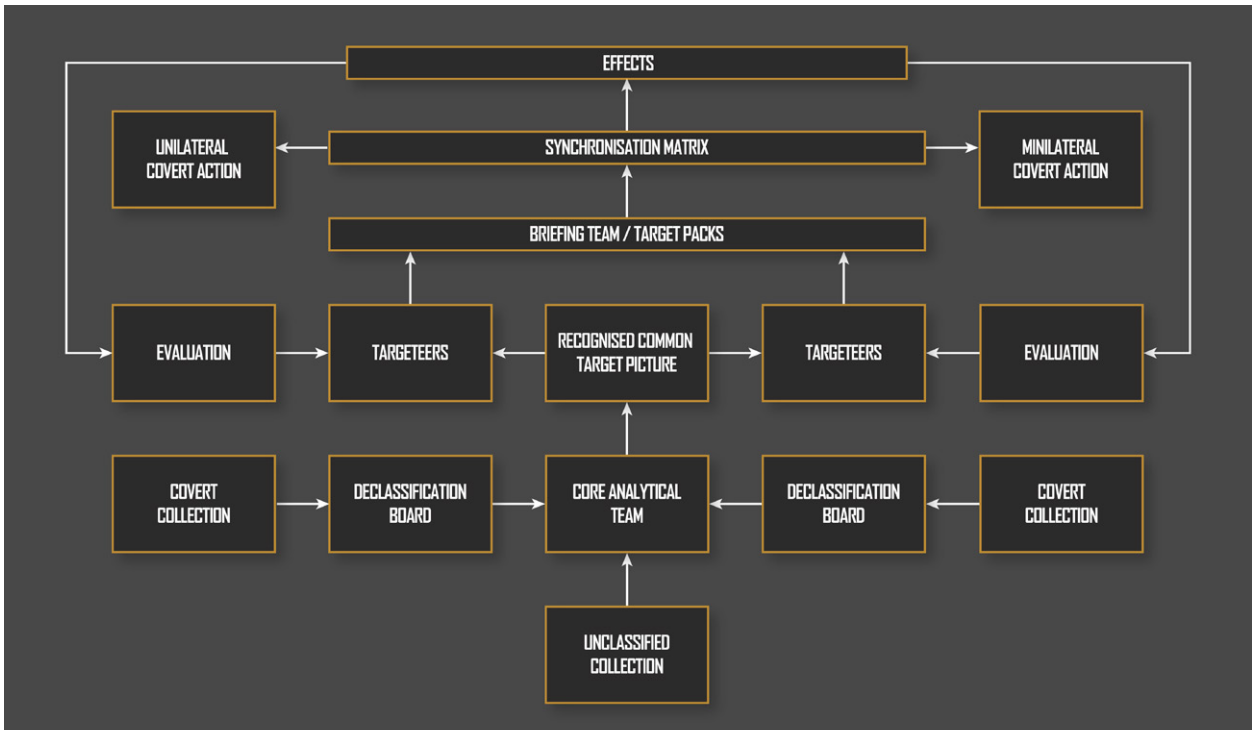
means where planning must be classified. Furthermore, different participating members may have quite different risk tolerances for what they are prepared to do unilaterally. Ukraine, for example, has no qualms about conducting kinetic operations. This is a problem that Western states have managed before. The US, for example, could collaborate with Israel on its efforts to constrain Iran's nuclear programme without participating in Israel's assassination programme targeting Iranian nuclear scientists.[135] Nevertheless, the question arises as to how the synchronisation process can function at the unclassified, the minilaterally classified and the unilaterally classified level. There is the risk, of course, that if multiple countries endeavour to conduct covert activities targeting the gaps in the synchronisation chart, that the effort could become fratricidal.

The layering of overt, covert and clandestine effects is achievable by participating states having an outline of the overt synchronisation matrix. There may also be occasional participants given observer status to the RCTP as a basis for their collaboration on effect delivery. Nevertheless, it becomes possible for states to work minilaterally or unilaterally away from the fusion centre to plan and execute effects, and to deconflict with others.

Another area for consideration is where the intent of a covert operation is to spike a Russian procurement process rather than to deny it. This could involve taking the money of Russian procurement agents and then failing to supply the goods, or providing microelectronics that are defective. If synchronised with disinformation suggesting that a procurement agent is defrauding their employer, these kinds of techniques can result in Russian enablers being targeted even if they are beyond the jurisdiction of the participating states. Attacking trust and confidence in Russian procurement processes is valuable because it forces validation mechanisms and frictions into all operations. However, to carry out such actions it becomes necessary for states to avoid having the fusion centre coordinating interdiction of the related shipments. A system of red flags – preventing interdiction of specific shipments – brings with it both the risk that the Russians are tipped off, and the potential for participating states to undermine the process by red-flagging actual targets. These issues can be managed, however, as they are similar to some of the methods used by law enforcement to target drug cartels. Again, minilateral explanation can enable appropriate handling of such opportunities.

135. See Ronen Bergman, *Rise and Kill First: The Secret History of Israel's Targeted Assassinations* (New York, NY: Random House, 2018), pp. 588–609.

Figure 6: The Workflow of the Multinational Fusion Centre



Source: Author generated.

The metrics of success for operations targeting Russia's defence industry will be harder to measure in open sources. The relevant metrics are: reduced production output of key weapons systems; reduced reliability of key weapons systems; or increased cost of production. The volume of weapons being fired is a poor and methodologically challenging proxy for any of these variables. Although they will correlate over time, there is often a considerable lag between disruption to production and shifts in use at the front. This makes it difficult to attribute cause and effect. The problem is that the metrics must necessarily derive from inside Russia's defence industry and are therefore likely to only be accessible via covert collection. How, therefore, can the fusion centre assess its impact?

In some respects, participating states will only continue to support the endeavour if they see a return on investment. That they each conduct damage assessments using their own collection capabilities therefore provides those funding the effort with internal validation of impact. This kind of data is often available from relatively low-level collection. Individually, the sourcing is highly sensitive, but once aggregated, it becomes difficult to attribute it to a source. To that end, it should be possible for participating states to declassify aggregated assessments relating to these metrics periodically, at intervals that allow for meaningful changes to be picked up.

Conclusions

If Russia can be stopped in Ukraine, the prospects for European security will immeasurably improve. If Russia achieves its objectives in Ukraine, the credibility of NATO's conventional deterrence posture becomes critical to the security of Europe. In either case, the industrial capacity of NATO states is important in ensuring that Ukraine can continue to fight or that NATO's forces are ready to deter. The strain, however, can be lessened by reducing Russia's capacity to arm and equip its forces. The extensive dependence of Russia's defence industry on international supply chains makes it vulnerable to disruption. Thus far, however, Ukraine's international partners have failed to significantly curb Russian defence production.

This paper has sought to identify the cause of this failure. Ultimately, it has concluded that Ukraine's international partners have been reactive rather than proactive in targeting Russian defence industries; have suffered from the over-classification of relatively low-level intelligence and have thus failed to properly empower the manufacturers of the goods they are trying to disrupt; and have had policy frameworks orientated around unrealistic expectations of what can be achieved. Despite this, the exposure of Russia's defence industry to international efforts at disruption was shown to be considerable. There are multiple stages throughout the production process where intervention, both overt and covert, can cause delay, degradation in quality, or a serious increase in cost to Russia's arms production.

The methodology proposed for increasing the effectiveness of efforts at disarming Russia is threefold:

1. It is necessary to have an unclassified and therefore releasable RCTP of Russia's defence industry, with mechanisms for sharing target packs among participating countries that fit with those countries' legal requirements for authorising interventions.
2. It is necessary to synchronise and layer effects, spanning multinational overt action, minilateral covert action and unilateral clandestine action, to cause Russia's defence industry to be maximally disrupted.
3. It is necessary that states use intelligence collection to assess impact and then aggregate the collected data to reduce the sensitivity of their conclusions, enabling these to be shared to refine the targeting process.

After two years of largely ineffectual and poorly cohered efforts, the time to act is now.

About the Authors

Jack Watling is Senior Research Fellow for Land Warfare at RUSI. Jack works closely with the British military on the development of concepts of operation and assessments of the future operating environment, and conducts operational analysis of contemporary conflicts. His PhD examined the evolution of Britain's policy responses to civil war in the early 20th century. Jack has worked extensively on Ukraine, Iraq, Yemen, Mali, Rwanda and further afield. He is a Global Fellow at the Wilson Center in Washington, DC.

Gary Somerville is a Research Fellow in RUSI's Open Source Intelligence and Analysis Research Group.