RUSI

Royal United Services Institute
for Defence and Security Studies

Founded in 1831
Patron Her Late Majesty the Queen
President HRH The Duke of Kent KG

James Byrne: Director of the Open Source Intelligence and Analysis (OSIA) department at the Royal United Services Institute (RUSI), London

Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations

27 February 2024

Introduction

Chair Blumenthal, Ranking Member Johnson, and distinguished Members of the Subcommittee. I am very honoured to be here today to present on the work of the Royal United Services Institute (RUSI) tracing Russian military supply chains. My name is James Byrne, and I am the Director of the Open Source Intelligence and Analysis (OSIA) department at RUSI in London.

RUSI is the world's oldest and the UK's leading defence and security think tank. Our mission is to inform, influence and enhance public debate to help build a safer and more stable world. Founded in 1831 by the Duke of Wellington, RUSI's primary mission was the study of military and naval sciences. Today, we have several departments working on many important issues centred primarily around questions of defence and security.

One of my team's important missions has been the generation of open-source actionable intelligence on Russia's military supply chains. Our aim, since the war began, has been to identify the people, companies and networks procuring microelectronics and other technology used by the country's military industrial complex. This is what I am here to speak about today, alongside other respected experts on this topic from the Kyiv School of Economics and Conflict Armament Research, two institutions that have led the field on this topic.

Russia's Quest for Western Technology

Since Russia's February 2022 invasion of Ukraine, the Armed Forces of the Russian Federation (AFRF) have deployed and used one of the world's largest arsenals of modern weaponry in what has proven to be a grinding attritional conflict that has cost hundreds of thousands of lives.

Because Russia's hubristic and irredentist designs did not proceed as planned, the Kremlin soon found itself expending and losing vast amounts of equipment, munitions and materiel. Battlefield losses included many of Russia's most sophisticated weapons, systems and platforms, including state-of-the-art air defence and electronic warfare systems, cruise missiles, precision munitions, unmanned aerial vehicles, encrypted communications systems, tactical radios and a wide range of other systems.

Soon after the beginning of the war, staff from the Royal United Services Institute (RUSI) – a defence and security think-tank in Whitehall London – gained access to many of these systems in Ukraine. Since then, RUSI staff have regularly visited the country and the facilities at which these weapons and platforms are disassembled and inspected. Over the course of this research, RUSI staff discovered that many of these systems are often built with, and reliant upon, Western technology.

In August 2022, we published out first report from this research, titled *'Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine'*.[1] In this report, we detailed at least 450 different kinds of unique foreign-made components across 27 different weapons and military systems, the majority of which were manufactured by US companies with a longstanding reputation for designing and building sophisticated microelectronics for the US military. Of these, at least 80 different kinds of components were subject to export controls by the US, indicating that Russia's military–industrial complex had, in recent decades, been able to successfully evade these. Surprisingly, many of the components used in these systems were commercial off-the-shelf-electronics, even those often used in high-end military platforms.

[1] RUSI, *'Silicon Lifeline Western Electronics At The Heart Of Russia's War Machine'*, < https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf>.

Figure 1: RUSI Public Reports on Ukraine

RUSI
Royal United Services Institute for Defence and Security Studies
The Plot to Destroy Ukraine
Jack Watling and Nick Reynolds
Special Report
15 February 2022
Operation Z
The Death Throes of an Imperial Delusion
Jack Watling and Nick Reynolds
Special Report
22 April 2022
Ukraine at War
Paving the Road from Survival to Victory
Jack Watling and Nick Reynolds
Special Report
4 July 2022
The Russian Air War and Ukrainian Requirements for Air Defence
Justin Bronk with Nick Reynolds and Jack Watling
Special Report
7 November 2022
Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023
Jack Watling, Oleksandr V Danylyuk and Nick Reynolds
Special Report
29 March 2023
Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine
Jack Watling and Nick Reynolds
Special Report
19 May 2023
SILICON LIFELINE
WESTERN ELECTRONICS AT THE HEART OF RUSSIA'S WAR MACHINE
JAMES BYRNE, GARY SOMERVILLE, JOE BYRNE, JACK WATLING, NICK REYNOLDS AND JANE BAKER
AUGUST 2022
THE ORLAN COMPLEX
TRACKING THE SUPPLY CHAINS OF RUSSIA'S MOST SUCCESSFUL UAV
JAMES BYRNE, JACK WATLING, JUSTIN BRONK, GARY SOMERVILLE, JOE BYRNE, JACK CRAWFORD AND JANE BAKER
DECEMBER 2022

Source: RUSI.

While these kinds of components play a huge number of different roles in commercial electronic systems, they also sit at the heart of how modern wars are fought. Complex sensors, information processing systems, targeting and navigation complexes, encrypted communication equipment and many other modern platforms rely for their very function on these kinds of microelectronics.

Since the summer of 2022, my team has generated dozens of private and public reports detailing the components found in other Russian weapons platforms and the supply chains through which these and other materials for its military industrial complex are moved.[2]

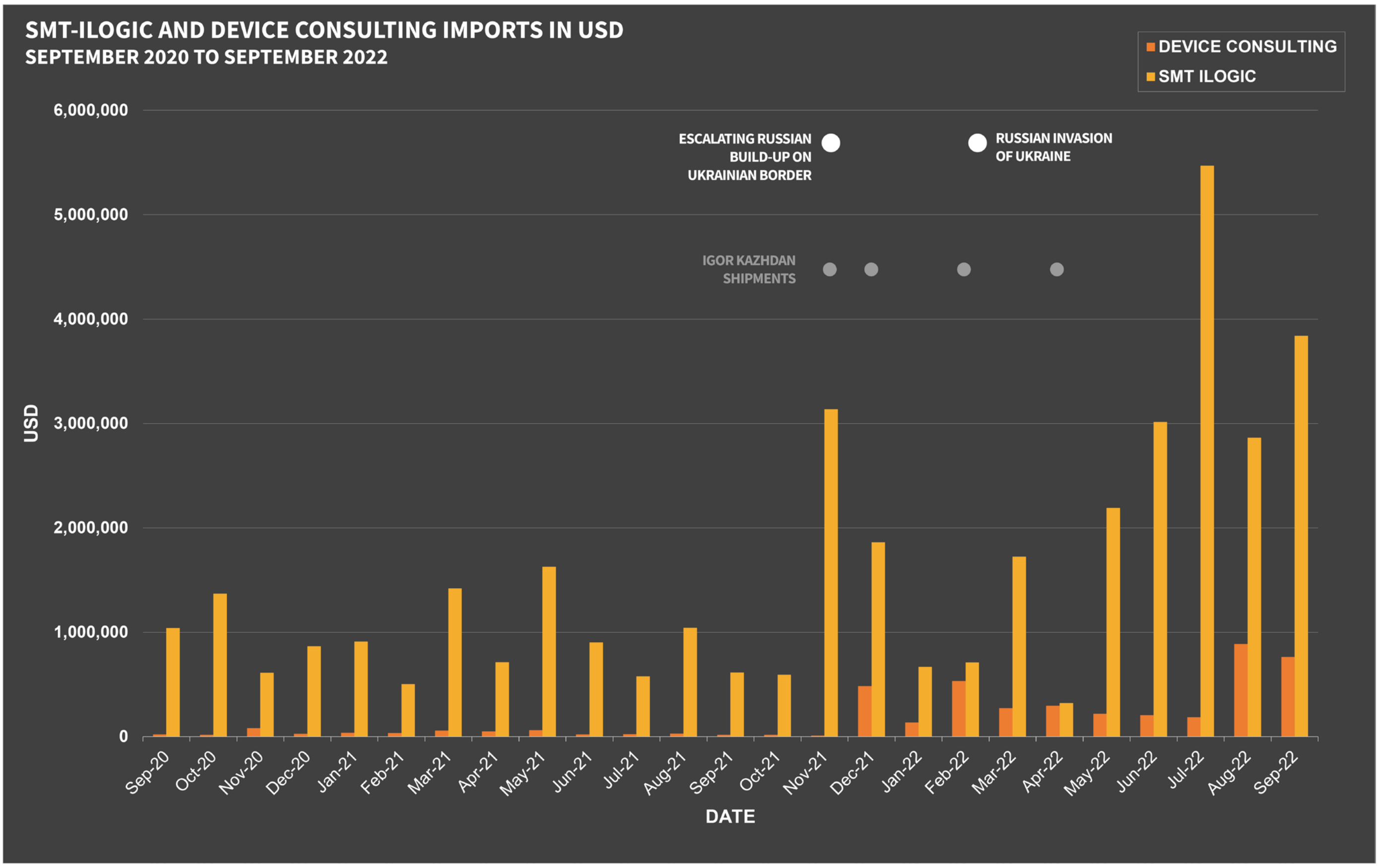
Unfortunately, our findings indicate that, in many cases, imports of microelectronics and other components into Russia increased drastically after the invasion of Ukraine.[3] Although wide-ranging sanctions and tighter export controls across Western countries sought to restrict the flow of these technologies to the country, Russian procurement networks adapted, routing shipments through third countries such as Hong Kong, China, Turkey, Uzbekistan, and the UAE.[4]

[2] RUSI, *'In Plain Sight Operations of a Russian Microelectronics Dynasty'*, < https://rusi.org/explore-our-research/publications/commentary/report-plain-sight-operations-russian-microelectronics-dynasty>.

[3] RUSI, *'The Orlan Complex Tracking The Supply Chains Of Russia's Most Successful UAV'*, < https://static.rusi.org/SR-Orlan-complex-web-final.pdf>.

[4] Carnegie Endowment for International Peace, *'Hong Kong's Technology Lifeline to Russia'* < https://carnegieendowment.org/2023/05/17/hong-kong-s-technology-lifeline-to-russia-pub-89775>.

Figure 2: Imports of Microelectronics by companies linked to the Orlan-10 UAV manufacturer.



Source: RUSI OSIA.

Today, Russia continues to import large volumes of microelectronics and other equipment needed to build, field and sustain the weapons it uses in its aggressive war in Ukraine. While fewer of these systems are recovered and disassembled than at the start of this conflict, technical exploitation of the systems that have been recovered shows that many of the components have been manufactured recently. In some cases, these are even export controlled components designed to facilitate AI computations for automated battlefield tracking, classification and targeting.

For the Russians, the procurement of microelectronics is a strategic priority. Without them, missiles cannot be guided to their targets, unmanned aerial vehicles (UAVs) cannot fly and communications systems cannot work. As a result, Russia and its special services invest a large amount of resources into building the logistical and financial networks to procure these technologies and move them across international borders. To do so they use cut-outs, front companies, fraudulent end-user certificates and other obfuscatory measures once pioneered by the KGB.

Several recent cases in North America[5] and Europe[6] show that Russian procurement networks are active in our countries and in various other parts of the world. We recently conducted a joint investigation with Dutch and German media outlets into one such case that involved illicit procurement networks snaking through Germany, Lithuania, and Hong Kong into Russia.[7]Sometimes, these networks are operated by trained Russian intelligence officers and people working on their behalf. In other cases, it is trade for purely pecuniary purposes by people with few scruples.

But this is not just a story about Western designed and manufactured microelectronics, because Russia's military industrial complex needs many different kinds of goods manufactured in our countries. Machine tools, ball bearings, carbon fibre and polymers, sensors, cameras, chemicals and many other kinds of goods are often purchased abroad and diverted to Russia's military industrial complex to manufacture the weapons the AFRF needs. As a result, the Kremlin's military supply chains are forced to stretch across the globe, often starting in North America or Europe and ending in military factories across Russia.

Conclusion

[5] U.S. Immigrations and Customs Enforcement, *'HSI investigation leads to OFAC sanctions, indictment charging Iranian national with unlawfully procuring microelectronics used in unmanned aerial vehicles'* <https://www.ice.gov/news/releases/hsi-investigation-leads-ofac-sanctions-indictment-charging-iranian-national>.
[6] Europol, *'Suspect arrested in the Netherlands for circumventing EU trade sanctions against Russia'*, <https://www.europol.europa.eu/media-press/newsroom/news/suspect-arrested-in-netherlands-for-circumventing-eu-trade-sanctions-against-russia>.
[7] RUSI, *'In Plain Sight Operations of a Russian Microelectronics Dynasty'*, < https://rusi.org/explore-our-research/publications/commentary/report-plain-sight-operations-russian-microelectronics-dynasty>.

As Russia faces the prospect of a protracted conflict in Ukraine, the Kremlin is increasingly gearing its economy for war. The Russian finance minister left little room for interpretation about Moscow's priorities when he said in October 2023 that 'the main emphasis is on ensuring [Russia's] victory – the army, defence capability, armed forces, fighters – everything needed for the front, everything needed for victory is in the budget'.

Hence, with Russia diverting all possible financial and technical resources to support its war of aggression, our countries should ensure that Western technology and microelectronics are not in Russia's arsenal. Today, U.S. and European technology is at the heart of Russian weapons used against the people of Ukraine. But tomorrow, these same systems could be used against us and our allies. We should, therefore, make it as difficult as possible for Russia and other adversaries to build their arsenals of war with the technologies we have designed and manufactured.

Thank you for the opportunity to give testimony here today.