STRIDER

NAVIGATING THE NEW GEOPOLITICAL REALITY

Understanding and Mitigating Russia's Evolving Economic Tactics

TABLE OF CONTENTS

INTRODUCTION

Russia is adapting its strategies to navigate economic isolation and sustain its technological edge amid the ongoing war in Ukraine. This shift is reshaping the geopolitical landscape. Sanctions and export controls imposed by the United States and its allies have disrupted traditional avenues for acquiring critical technology, driving the Kremlin to evolve its tactics in response. As Russia refines its methods—from reverse engineering Western-made products to leveraging international relationships for gray zone operations, it poses increasingly complex challenges.

> **The need for strategic intelligence has never been greater.**

The reshaping of the geopolitical landscape means that new actors, such as the private sector, have an increased role in countering adversarial nations. From protecting sensitive technology from sanction evasion schemes to combatting changing economic espionage tactics, organizations need to take a proactive security posture. As Western governments put more responsibility on the private sector to protect their technology, **organizations need the right tools to navigate this intricate landscape.**

In the following section, we'll dive deeper into these findings with four reports written by Strider's Global Intelligence Unit, each offering a comprehensive view into how Russia is adapting its tactics. The intelligence in this document is derived from Strider's proprietary methodology, which utilizes exclusive data sources and advanced analytics to deliver unparalleled insights into the Kremlin's evolving strategies.

RUSSIA ADAPTS ECONOMIC ESPIONAGE TACTICS IN EUROPE

Shifting Strategies Amid Heightened Demand for Foreign Technology

The war in Ukraine, combined with the resulting economic and diplomatic isolation, has intensified Russia's need for foreign technology and expertise, prompting shifts in how it seeks these resources across Europe. In response, the Kremlin has doubled down on its goal of achieving "technological sovereignty," focusing on import substitution and developing a domestic technology base to support ongoing advancements despite foreign restrictions.

Russia has lost
50,000 SCIENTISTS
to emigration since 2019

Sanctions and export controls imposed by the US and its allies have deprived Russia of many dual-use products crucial to sustaining its longer-than-anticipated war in Ukraine. The struggle to acquire other critical technologies—such as quantum computing, additive manufacturing, and augmented reality—is causing Russia to lag further behind the West.

Russia's technology sector is also suffering from a significant brain drain. Since the invasion, around one million Russians—most of them young, well-educated individuals who would have contributed to Russia's advanced industries—have fled the country, according to the French Institute of International Relations. In 2023, the Vice President of the Russian Academy of Sciences estimated that Russia has lost 50,000 scientists to emigration since 2019.

Disruption of Traditional Espionage Methods in Europe

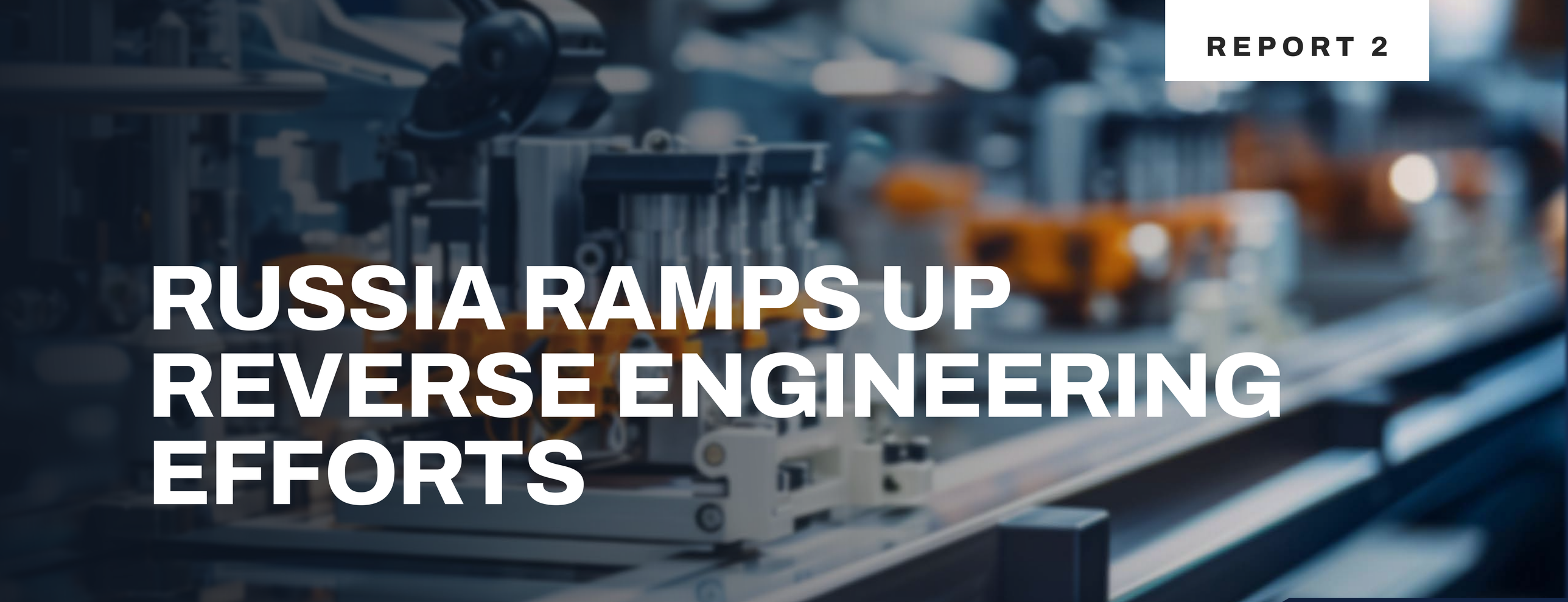
In Europe, Russia's traditional intelligence and technology-gathering operations have been severely disrupted by diplomatic expulsions and travel restrictions. The expulsion of Russian officials, including intelligence officers, has significantly reduced the number of personnel able to engage in economic espionage on the continent.

- Since the full-scale invasion in 2022, more than 700 Russian officials have been expelled from their host countries, mostly in Europe. At least eight European nations have closed Russian diplomatic facilities.
- Europe has also implemented visa restrictions on Russian citizens and banned Russian airlines from European airports and airspace, further limiting Moscow's ability to conduct espionage activities.

Evolving Tactics to Achieve Technological Sovereignty

As a result, Russian intelligence services are shifting to new strategies and techniques to obtain the European technology and expertise needed to close the gap and achieve "technological sovereignty." These adaptations include a growing reliance on individuals operating under non-official cover, such as oil and gas workers, professors, and other professionals, according to European media reports.

- To compensate for reduced opportunities for in-person contact, Russian operatives are increasingly turning to social media platforms like LinkedIn to connect with targets in Europe and the United States.
- Moscow is also leveraging the Russian academic diaspora and its international connections to further its economic statecraft objectives. In 2023, Vladimir Putin ordered the resumption of the "Mega Grant" program, which recruits foreign scientists to conduct research at Russian labs. That same year, Russia launched a program to collect information on experts attending international scientific conferences and events



RUSSIA RAMPS UP REVERSE ENGINEERING EFFORTS

Government Funding Fuels Reverse Engineering Initiatives

Since 2022, the Russian government has funneled at least USD 110 million into projects focused on reverse engineering Western-made products. This has raised concerns that foreign companies may face increased competition from Russian knockoffs in markets favorable to Russia, such as India. This push also bolsters the Russian military's potential to employ imitation technology.

The Russian government is targeting hundreds of products manufactured by leading American and European companies for reverse engineering

Last year, Russian President Vladimir Putin directed the government to use funds from the "exit tax" imposed on foreign companies leaving Russia to finance reverse engineering initiatives. This decision positions these projects as a form of retribution against firms that chose to exit the country following Russia's full-scale invasion of Ukraine.

The Russian government is targeting hundreds of products manufactured by leading American and European companies for reverse engineering, including integrated circuits, chemical compounds, automotive parts, and engines.

Strategic Integration of Reverse Engineering and Intelligence

Russia's emphasis on reverse engineering underscores the value Moscow places on acquiring trade secrets and creates opportunities for closer collaboration between private industry and the Russian intelligence community. Proprietary knowledge of manufacturing processes, for instance, would be invaluable for replicating complex machinery, such as aircraft engines—one of the key targets for Russian reverse engineering efforts.

- Two universities at the forefront of implementing these reverse engineering projects and providing training to Russian companies have been previously implicated in economic espionage activities, according to Western media reports.
- In 2010, Putin proposed merging Russia's intelligence services with private industry to reduce reliance on Western goods in the energy sector. Since then, the government has launched various initiatives, including a state-supported plan backed by Gazprom Neft to establish a federal reverse engineering center.

Defense Sector Prioritization and International Collaboration

The desire to replicate Western weapon systems is likely a primary driver behind Russia's investment in reverse engineering. Russian military officials, legislators, and Putin himself have expressed support for reverse engineering NATO military equipment captured in Ukraine.

- The defense industry has been given priority access to these reverse engineering resources, according to the deputy head of a Russian agency responsible for allocating grants to such projects.
- Russia's expanding reverse engineering capabilities could pave the way for increased cooperation with Iran. According to Western news reports, Russia has shipped Western military equipment seized in Ukraine to Iran for analysis, indicating a potential exchange of technical knowledge between the two countries.

RUSSIA LEVERAGING RELATIONSHIPS FOR GRAY ZONE OPERATIONS

Exploiting Individuals in Europe for Malign Activities

Russia is using individuals living in Europe to target infrastructure and organizations—especially those providing support to Ukraine—as part of a broader campaign that includes intelligence gathering and schemes to evade sanctions. These “gray zone” operations, which stop short of open conflict, involve activities such as arson, attempted bombings, vandalism, and other disruptive actions intended to create chaos and undermine NATO and EU cohesion.

The German domestic intelligence agency assessed in April that there was a significantly heightened risk of Russian-directed sabotage.

In May, NATO issued a statement condemning Russia’s sabotage and other malign activities across Europe. The German domestic intelligence agency assessed in April that there was a significantly heightened risk of Russian-directed sabotage.

In May, European authorities linked Russia to a series of incidents across the continent, including an arson attack on a Ukrainian-linked warehouse and the jamming of civil aviation GPS systems. Earlier in the year, German and US authorities thwarted the assassination of an executive at a German company providing support to Ukraine.

Leveraging Ideological Ties and Online Profiles for Manipulation

Moscow is leveraging the ideological, political, or personal ties of individuals to Russia for these operations. The Russian government reportedly analyzes online profiles of individuals in Europe to identify those who may be susceptible to manipulation by the Kremlin. Additionally, Russian media reports suggest Moscow may be utilizing black-market databases of individuals who have moved abroad since the war in Ukraine began.

In June, a university professor in Estonia was found guilty of espionage for providing Russia with the identities of individuals capable of influencing Estonia's domestic, foreign, and security policies. The professor had previously been employed by a Russian university and traveled to Russia to attend academic events.

In 2023, German authorities arrested a dual Russian-German citizen for exporting military goods to Russia. The individual was a leader in a political association closely tied to Russian-backed separatist forces in Ukraine, according to a Russian media report.

EU TO BEGIN NEW RUSSIA SANCTION EVASION ENFORCEMENT

New prohibitions on exports to Russia will raise compliance burdens and risks for EU-based businesses. The requirement, which will be enforced starting in January 2025, is the latest in a series of restrictions, and will require exporters to include a "No Re-Exports to Russia" clause in contracts.

- EU businesses were given a year transition period to include this clause in contracts for certain restricted goods, such as dual-use items, advanced technology used by the Russian military, and aviation items.

- Since Russia's full-scale invasion of Ukraine in 2022, the EU and its allies have implemented hundreds of sanctions aimed at limiting Moscow's access to foreign technology necessary to sustain the war, but third-party countries continue to play a key role in sanctions evasion.

The latest restriction requires EU businesses to conduct "adequate due diligence measures" to establish the end users of their products. Although the new regulation did not specify a penalty for breaking the clause, EU legal experts assess that member states will set and enforce penalties for breaches.

Adopting good due diligence processes is especially important for organizations operating in areas posing a high-risk of circumvention, such as the PRC, Turkey, and other countries with close relations with Russia.

These organizations should also enhance monitoring systems and reporting mechanisms to ensure that protocols are in place if a breach of contract is identified.

Enhanced Guidance and Compliance Measures

In late September 2024, the U.S., UK, Canada, France, Germany, Italy, and Japan published updated guidance for industry to prevent Russia from evading export controls and sanctions.

- The guidance recommends beginning with sanctions list checks, though Strider's analysis shows these lists cover only a small fraction of entities likely involved in extensive sanctions-evasion networks.
- The guidance also encourages companies to perform due diligence on their supply chains, such as monitoring addresses added to the U.S. Department of Commerce's Entity List.

Shifting Responsibility to the Private Sector

Although governments have put new guidance and regulations in place, the current strategy still falls short to curb Russia's access to foreign technology. As seen above, Western governments have shifted responsibility to the private sector to vet their supply chains to stop the flow of products to Russia. However, the private sector often lacks the resources and expertise to conduct effective supply chain analysis and relies heavily on sanctions and export control lists, which overlook the many entities involved in sanctions-evasion networks. As a result, according to Ukraine's military intelligence agency, there has been no significant change in the flow of foreign components to Russia.

CONCLUSION

As Russia adapts its methods to acquire foreign technology and sustain its economic resilience, the need for organizations to understand and navigate these evolving threats has become critical.

This complex environment requires more than traditional due diligence or surface-level risk assessments.

Organizations must have a comprehensive understanding of how state actors, like Russia, manipulate supply chains, leverage global networks, and exploit access to sensitive technology.

STRIDER SOLUTIONS

Navigating Geopolitical Complexity with Unmatched Strategic Intelligence

As geopolitical tensions and economic strategies evolve at an ever-increasing rate, organizations face unprecedented challenges in protecting their supply chains and critical technologies. Strider's Checkpoint solution is designed to empower companies with the strategic intelligence needed to navigate these complexities effectively.

Checkpoint provides unparalleled visibility into complex supply chains, uncovering hidden connections to state-sponsored actors and high-risk entities. By leveraging advanced analytics and exclusive data sources, Checkpoint enables organizations to proactively identify and mitigate risks that standard due diligence processes may overlook. This is especially critical in the context of Russia's evolving tactics to acquire foreign technology despite extensive sanctions.

Amid the growing complexities of global trade and geopolitical risk, having a tool like Checkpoint is essential for any organization aiming to maintain operational integrity and protect its technological assets from state-sponsored risks.

Discover how Checkpoint and Strider's full product suite can help you better navigate these challenges and secure your organization at striderintel.com.

striderintel.com/request-demo

HOW CHECKPOINT ADDRESSES CURRENT GEOPOLITICAL CHALLENGES:

SUPPLY CHAIN TRANSPARENCY

Checkpoint uncovers hidden supplier relationships, including those tied to sanctioned or high-risk entities, ensuring that businesses can safeguard their operations against inadvertent involvement in sanctions-evasion networks.

ENHANCED COMPLIANCE

By providing accurate, up-to-date intelligence on third-party risks, Checkpoint streamlines compliance efforts, helping organizations align with regulatory requirements and avoid reputational damage.

PROACTIVE RISK MANAGEMENT

With insights into the economic ties and activities of entities within Russia's defense industry, organizations can make informed decisions to preemptively block potential threats, rather than reacting to them after exposure.

This report was sourced using a combination of Strider's proprietary data sources as well as open-source data. Reach out to our team via email at **info@striderintel.com** with questions about source information or methodology.