MANAGING RISKS CREATED BY RUSSIA'S INVASION OF UKRAINE: ENHANCED DUE DILIGENCE AND ADVANCED KNOW-YOUR-CUSTOMER POLICIES

The Russian war machine, though hampered by Ukrainian resistance, logistical issues, and Western sanctions, continues to attack civilians and civilian infrastructure. Much of the Russian ammunition, drones, and other military equipment are made using imported components, which Russia continues to acquire by utilising different sanction circumvention schemes. Civil society organisations and open-source intelligence research groups have analysed these schemes and supply chains, identifying a wide range of components sourced from Western manufacturers and used in Russia's full-scale invasion of Ukraine.

Businesses have a responsibility to ensure they do not cause, contribute to, or are linked to human rights harms. There are serious legal, reputational, and regulatory risks for businesses whose components end up in Russian weapons used in violations of international law. To manage these risks, businesses must strengthen their human rights and know-your-customer (KYC) due diligence processes. At the same time, policymakers must update supply chain due diligence guidelines to ensure businesses operating in their jurisdictions do not unknowingly undermine sanctions placed on Russia and contribute to gross violations of human rights and humanitarian law.

RECOMMENDATIONS

- Companies must allocate resources and put in place appropriate internal mechanisms and tools to empower their risk assessment departments to carry out enhanced due diligence of supply chains, intermediaries, customers, and end-users.
- Companies must review their supply chain risk matrix to optimise their procedures for the regions that have been identified as emerging hubs for sanction diversion and circumvention and conduct enhanced due diligence during the onboarding of any new suppliers in these regions.
- Companies must conduct a detailed review of the policies and procedures of their customers to ensure that they are able to prevent re-exports for military end-uses in Russia.
- Companies must take into account potential red flags that consider the use of front companies by illicit networks to obfuscate the true end-user of products and evade sanctions and export controls.
- Companies should collaborate with civil society experts to develop an industry standard-setting process and better monitoring, identification, and mitigation of risks.
- Companies must create mechanisms for information exchange with governments and civil society groups to better investigate existing illicit networks and paths for components re-export to Russia and identify ways to disrupt them.

Last updated: September 2023

- Companies must establish internal policies and procedures that enable them to rapidly investigate and respond in cases where their components are reported to have been integrated into military equipment used by Russia in Ukraine.

RED FLAGS IN A POST-FEBRUARY 2022 WORLD

Non-Russian front companies used to supply Russia with Western components often share several commonalities that are potential red flags:

1. Recent registration – particularly in the months following February 2022;
2. Registration in known transhipment hubs, where it is easy to register a business, where there are lax export controls, and where there are either porous borders with Russia or a prior history of serving as a transhipment point for Russia;
3. Minimal share capital, despite making large orders of products within a short space of time;
4. No physical office, for example, listing the address of corporate secretary services providers instead, or being registered in disused, rundown, or residential buildings;
5. Share an address with other companies or share contact details with sanctioned or previously identified Russian military-affiliated companies;
6. Obscure beneficial ownership and shareholding structures, for example, with owners in secret or opaque jurisdictions;
7. List nominal shareholders and directors that are either (a) also listed in similar roles in dozens of other companies or (b) low-profile individuals who have no other businesses or track record of working in the industry;
8. List Russian officials, former officials and/or their family members as directors and/or shareholders;
9. Have either no website, or a website only in Russian language, or a domain name registered by a Russian entity;
10. Have a historic business relationship with Russian entities – particularly military-affiliated – or have continued to ship large amounts of microelectronics or other dual-use goods to Russia;
11. Evidence of shipments of microelectronics or other dual-use goods to Russia since February 2022, despite not having done so before.

TOOLS

There are several tools available to assist companies in identifying potential red flags and enhancing human rights and KYC due diligence processes:

- Refinitiv is a financial software that can provide the necessary capability to conduct risk and compliance analysis of supply chains. Its database can uncover hidden risks in business relationships and human networks, identifying high-risk or sanctioned entities and individuals.
- Sayari Analytics is a financial intelligence platform allowing users to investigate ultimate beneficial ownership of companies and identify potential links to illicit activities and sanctioned entities. Sayari database can be used to build models of commercial and financial relationships to map out networks of companies linked by common identifiers across multiple jurisdictions.

- Altana Trade Atlas is a dynamic AI platform that uses public and non-public data to enable greater visibility in supply chains across the globe. Altana conducts threat network analysis and AI targeting across global supply chains and business networks, to identify illicit network and trade activity.
- OECD Due Diligence Guidance for Responsible Business Conduct - this guidance describes the due diligence process and supporting measures in a step-by-step fashion and can help set up due diligence processes or improve existing processes.
- A Due Diligence Toolbox for SMEs, consisting of a self-assessment tool and an online practical manual, can be helpful for smaller companies looking to improve their due diligence processes**.**

RED FLAGS IN ACTION: ANONYMIZED CASE STUDIES

The following case studies showcase the importance of conducting enhanced know-your-customer (KYC) due diligence processes to obstruct sanctions evasion schemes:

CASE STUDY 1: COMPANY A approached a dual-use component manufacturer/supplier to acquire several components, which are manufactured in the EU and are specifically designed for a Russian vehicle that has military and civilian models. COMPANY A is registered in an Asian country, and its director, PERSON B, is a Russian national living in the USA. The manufacturer/supplier agreed to the sale. However, by carrying out the enhanced due diligence that an entity with the red flags possessed by COMPANY A requires, the manufacturer/supplier would have found that:

- Since February 2022, COMPANY A has sent numerous shipments of dual-use components to Russia.
- PERSON B is also the founder and sole owner of a Russian company, COMPANY C.
- COMPANY C has won numerous contracts with Russian state entities to supply components similar to those shipped by COMPANY A from the Asian country.

PERSON B's links to a company that was directly supplying the Russian military-industrial complex are a major source of concern and highlight the risk that this trade of dual-use components was diverted to evade sanctions.

CASE STUDY 2: COMPANY D, registered in a Middle Eastern country after February 2022, approached a supplier of a chemical that is critical to the manufacture of certain military items and the production of electronic components required for weapons systems. The director of COMPANY D, PERSON E, is a Russian national. The chemical supplier agreed to the sale. However, by carrying out the enhanced due diligence that an entity with the red flags possessed by COMPANY D requires, the supplier would have found that:

- COMPANY D has shipped a large volume of chemicals to Russia since February 2022.
- PERSON E is the spouse of PERSON F, a high-profile businessperson in Russia. Amongst many other corporate affiliations, PERSON F is also the director and sole owner of COMPANY G in Russia.
- COMPANY G has won dozens of contracts with Russian state entities, including the Russian Ministry of Defence. These contracts also include the supply of the same chemical that COMPANY D has shipped to Russia.

PERSON E's links to PERSON F and COMPANY G, which trades directly with the Russian Ministry of Defence, underscore the importance of considering family members, especially spouses, of company directors. The chemical supplier should have conducted enhanced due diligence, given the risk that this trade was diverted to evade sanctions.

CASE STUDY 3: COMPANY H, registered after February 2022 in COUNTRY K, located in the Middle East, approached a manufacturer/supplier of machine tools to acquire several products. The director of COMPANY H, PERSON L, is a Russian national who has a common name and a low public profile. The manufacturer/supplier agreed to the sale. However, by carrying out the enhanced due diligence that an entity with the red flags possessed by COMPANY H requires, the manufacturer/supplier would have found that:

- COMPANY H has shipped a large volume of EU-manufactured machine tools to Russian COMPANY J since February 2022. COMPANY J is a supplier of machine tools and components to Russia's military-industrial complex, having won dozens of contracts with Russian entities.
- The website of COMPANY H was registered by an email address with the same surname as PERSON L. This email address is also associated with the Russian-registered COMPANY M.
- COMPANY M's website advertises trade in sanctioned goods, stating that COUNTRY K is the best trade route for evading EU sanctions, and advertises warehouses and logistics routes across Europe, China and elsewhere. COMPANY M's website also advertises exports on behalf of Russia's military-industrial complex.
- The director and sole owner of COMPANY M is PERSON N, who is the spouse of PERSON L, the director of COMPANY H.

PERSON L's links to COMPANY M, which openly advertises its sanctions evasion capabilities, highlight the importance of identifying the corporate affiliations of directors as an integral part of the enhanced due diligence process. This would reduce the risk of machine tools sent to COUNTRY K being diverted to Russia and its military-industrial complex.

ABOUT THE AUTHORS

- The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank
- The Open Society Justice Initiative (OSJI) is a global program that utilises the law to promote and defend justice and human rights.
- The Independent Anti-Corruption Commission (NAKO) is a civil society organisation aimed at advancing good governance in the areas critical for Ukraine's national security.
- Heartland Initiative is a non-profit practice-based research organisation that supports the fundamental rights and freedoms of people impacted by armed conflict.