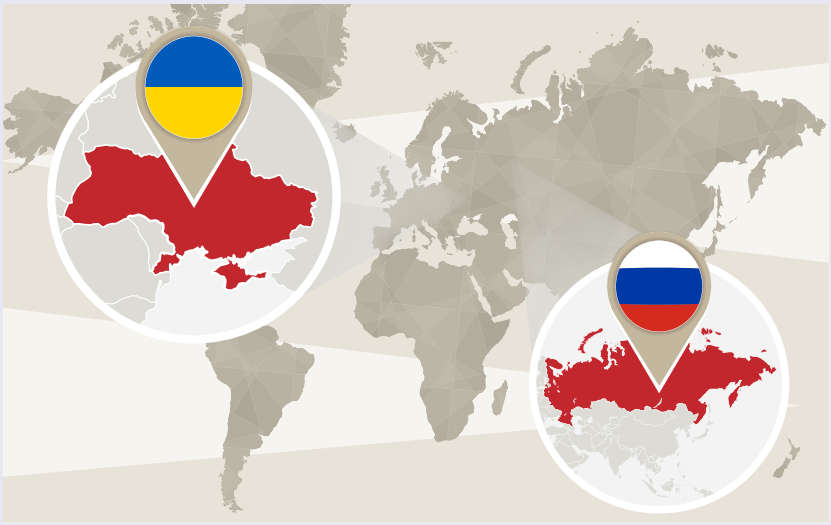
interos

Read Report

Supply Chain Disruption from the Russian Invasion of Ukraine



The Russian invasion of Ukraine is already beginning to cause extensive and debilitating supply chain disruption across the globe. This may result in rising input costs to a heightened threat of cyber-attacks, among other disruptions.

Russia, Ukraine key to global economy

Today thousands of U.S. and European companies do business with suppliers in Russia and Ukraine. Many of them could be at risk during a prolonged war. Analysis of global relationship data on the Interos platform reveals critical findings:

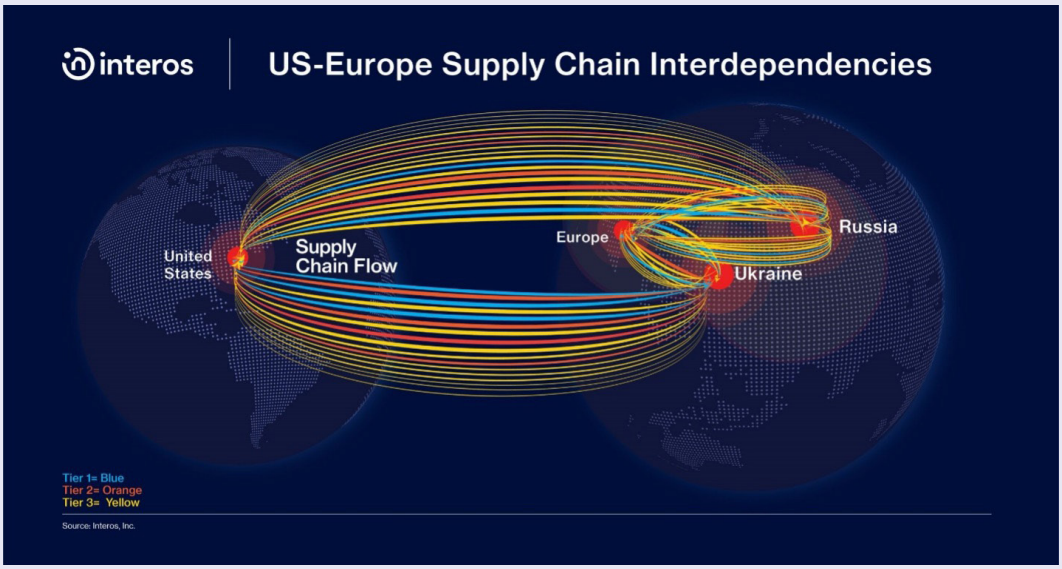
- More than 2,100 U.S.-based firms and 1,200 European firms have at least one direct (tier-1) supplier in Russia.
- More than 450 firms in the U.S. and 200 in Europe have tier-1 suppliers in Ukraine.
- Software and IT services account for 13% of supplier relationships between U.S. and Russian/Ukrainian companies. Consumer services represent another 7%. About 6% account for trading and distribution services and 4% for industrial machinery. Oil, gas, steel and metal products account for other everyday items purchased from the two countries.

The proportion of U.S. and European supply chains that include tier-1 Russian or Ukrainian suppliers is relatively low. This increases substantially when incorporating indirect relationships with suppliers at tier 2 and tier 3.

- More than 190,000 firms in the U.S. and 109,000 firms in Europe have Russian or Ukrainian suppliers at tier 3.
- More than 15,100 firms in the U.S. and 8,200 European firms have tier-2 suppliers based in Ukraine.

Supply chain and information security leaders in U.S. and European organizations should review their dependence on Russian and Ukrainian suppliers at multiple tiers. This is a key first step in assessing risk exposure in the region and ensuring operational resilience.

Supply Chain Disruption: 4 Major Risks



The war in Ukraine has the potential to spark supply chain disruption in four major areas:

Commodity price increases

Energy, raw material and agricultural markets all face uncertainty as the region descends into war. Russia provides over a third of the European Union's natural gas, and threats to this supply could force up prices when companies and consumers are already facing higher energy bills. Natural gas supply pressures are already spiking volatility in other energy markets too. By one estimate, the invasion could send oil prices spiraling to $150 a barrel, lowering global GDP growth by close to 1% and doubling inflation. Even lower estimates of $100 a barrel would cause input costs and consumer prices to soar.

Food inflation is another risk that may cause supply chain disruption. Ukraine is on track to being the world's third-largest exporter of corn, and Russia is the world's top wheat exporter. Ukraine is also a top exporter of barley and rye. Rising food prices would only be exacerbated with additional price shocks, especially as Russian loyalists seize core agricultural areas in Ukraine.

The invasion could continue to squeeze metal markets. Russia controls roughly 10% of global copper reserves and is also a significant producer of nickel and platinum. Nickel has been trading at an 11-year high, and further price increases for aluminum are likely with any disruption in supply caused by the war.

Firm-level Export controls and sanctions

U.S. and European export controls could exacerbate commodity cost pressures. The use of such controls to restrict certain companies or products from supply chains has soared over the last few years. While many have been aimed at Chinese companies, a growing number of Russian firms have been earmarked for export controls for "acting contrary to the national security or foreign policy interests of the United States."

Not surprisingly, U.S. companies and business groups are urging the government to be cautious in how it applies any new rules. Prior to the invasion, prominent Russian companies on a U.S. restrictions list included Rosneft and subsidiaries, and Gazprom. Following the Russian invasion of Ukraine on Thursday, the UK and US governments announced more significant and sweeping sanctions against major Russian banks. Extending export controls and sanctions to Gazprom's subsidiaries, other energy producers, and key mining and steel market firms could further impact supply availability and input costs.

U.S. and E.U. export controls are already targeting the Russian financial sector, including state-owned banks as a deterrence tactic. U.S. officials have noted that most sanctions are being aimed at the Russian financial sector for a "high impact, quick action response."

Cyber security collateral damage and supply chain turmoil

Entities linked to malicious cyber activity may also face further repercussions from the U.S. and its partners. Ukraine is certainly no stranger to Russian cyber aggression. Russia has twice disrupted the Ukrainian electric grid, first in December 2015, leaving hundreds of thousands of Ukrainians in the cold, and again the following year. But destructive attacks on the country's infrastructure could also spark significant collateral damage in global supply chains.

In 2017, the NotPetya attack on Ukrainian tax reporting software spread across the world in a matter of hours. The attack disrupted ports, shut down manufacturing plants, and hindered the work of government agencies. The Federal Reserve Bank of New York estimated that victims of the attack, including Maersk, Merck and FedEx, lost a combined $7.3 billion.

This figure could pale compared to the global supply chain impact of the Russia-Ukraine war, which will inevitably include a cyber element. Whether Russia would target its cyberwar playbook at U.S. or E.U. targets in retaliation for any support to Ukraine remains hotly debated. But the Cybersecurity Infrastructure and Security Agency (CISA) has been urging U.S. organizations to prepare for potential Russian cyberattacks, including data-wiping malware, illustrating how the private sector risks becoming collateral damage from geopolitical hostilities.

Geopolitical instability

Cyberwarfare is unlikely to remain within Ukraine's borders. Thus the destabilizing effect of a Russian invasion could have wider geopolitical ramifications. In Europe, a refugee crisis could emerge, with three to five million refugees seeking safety from the war. In Africa and Asia, rising food prices could fuel popular uprisings. Of the 14 countries that rely on Ukraine for more than 10% of their wheat imports, the majority already face food insecurity and political instability.

China is watching closely to see how the world responds if Russia invades Ukraine. The superpower has its own aspirations of seizing territory and extending its sphere of influence. Taiwan's defense minister has remarked that tensions over Taiwan are the worst in 40 years. The Russian invasion could further embolden China to enlist military tactics against Taiwan. In addition to far-reaching geopolitical implications, this will have a significant impact on electronics and other global supply chains.

How to Stop Supply Chain Disruption

Many of these risks are already materializing. But executives should think carefully about the impact of the Russia-Ukraine war. These leaders need to ensure appropriate contingency plans for their most critical supply chains and riskiest suppliers in the region.

Risk mitigation strategies include:

- evaluating required levels of inventory and labor in the short to medium term;
- discussing business continuity plans with key suppliers; and
- preparing to switch to, or qualify, alternative sources for essential products and services.

With proper analysis, planning, and execution, it is possible to mitigate significant risk, ensure operational resilience, and avoid supply chain disruption.

For more information:
www.interos.ai or **+1 703.677.3135**