LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What 2 Years Of Ukraine-Russia Conflict Can Teach Cos.

By **David Plotinsky, Vasilisa Strizh and Vishnu Shankar** (March 18, 2024, 5:57 PM EDT)


David Plotinsky


Vasilisa Strizh


Vishnu Shankar

It's now over two years since the ongoing conflict in Ukraine escalated, leading many companies with business operations or personnel in Eastern Europe to adjust, restructure or exit locations in Russia.

Meanwhile, the global business community has adapted to trade restrictions and sanctions, settled contract disputes and force majeure issues, prepared for and responded to cybersecurity breaches, and navigated challenges to the supply chain.

With continued political instability and military action occurring around the world, we review some of the key legal lessons learned from the Ukraine conflict.

Sanctions and Countersanctions

Although opinions are mixed on the overall effectiveness of sanctions as a response to Russia's actions against Ukraine, sanctions will very likely remain a key tool for many governments — including the U.S., U.K. and the European Union — in responding to global conflicts.

Russia sanctions also showed the willingness of the U.S. government to directly sanction persons that are foreign to a targeted country engaged in a conflict if they are abetting circumvention of the restrictions.

The Ukraine conflict saw increased coordination among U.S. government agencies, as well as the U.S. government and other countries' governments. This experience has likely created muscle memory that will facilitate such coordination in future conflicts.

While Russia sanctions have received significant recent attention, comprehensive sanctions programs exist for Cuba, Iran, North Korea and Syria, and the regions of Crimea and the Luhansk People's Republic and Donetsk People's Republic. Extensive sanctions are also in place for Venezuela and China.

The sanctions imposed on Russia by many countries and international bodies due to the conflict were in many ways exceptional in their coordination, breadth and speed. Therefore, with respect to Russia, as well as any future conflicts that may result in sanctions, even companies without U.S. connections should be prepared for the possibility of similar sanctions imposed by other countries.

Additionally, because international sanctions are unlikely to not mirror U.S. sanctions completely, even if there is some overlap — as is the case with the Russia sanctions — companies should ensure that their various transactions are evaluated against applicable programs.

Furthermore, sanctions can lead to contract performance issues that may result in arbitration or litigation.

In response to the sanctions imposed by other countries, and to the capital flight after the Ukraine conflict began, Russia introduced unprecedented restrictive measures known as countersanctions.

The countersanctions are designed to prohibit many actions and transactions with, or for the benefit of, persons from the so-called unfriendly countries, namely the U.S. and others that imposed sanctions against Russia.

Countersanctions restrict or block the ability of an unfriendly person to exit from its Russian business or investment, contain the export of capital, counter trade restrictions and withdraw intellectual property protections. Some have already resulted in Russia's appointed persons taking control of several businesses or projects owned by unfriendly persons.

The Ukraine conflict shows that affected companies must be prepared to navigate the complex and conflicting web of sanctions and countersanctions, and make difficult business decisions.

In a similar vein, the potential for that sort of retaliation should be considered as a risk factor when companies are assessing whether and how to invest in countries that are less stable and therefore may be at higher risk for conflicts that lead to sanctions and retaliatory responses.

While sanctions may be the regulatory response most directly tied to global conflicts, other tools at the disposal of the U.S. include export controls, import restrictions and foreign direct investment review.

Companies should be prepared for the possibility that otherwise acceptable transactions may be scrutinized more closely, or be subject to new and heightened restrictions, if they have a nexus to a country with an increased risk profile due to ongoing conflict or the increased likelihood of conflict.

These regulatory regimes involve compliance monitoring and enforcement by the government, which has been increasingly active on this front. It is therefore important that companies have sufficient compliance programs, with tools to avoid even inadvertent violations that can result in civil and criminal penalties, as well as reputational injury and other harm.

Contract Disputes

The Ukraine conflict resulted in the disruption of innumerable corporate, commercial and financial contracts, including those requiring performance by or with sanctioned entities, or otherwise affected by sanctions.

This is certainly not the first time — and won't be the last time — that international sanctions have played a role in litigation or arbitration over contract performance issues.

In response to the geopolitical situation, Russia adopted a law allowing a Russian court to accept

jurisdiction over disputes involving Russian sanctions or disputes otherwise related to sanctions, or where a matter is governed by laws of a country that introduced sanctions.

Sanctions have led parties to invoke force majeure and termination provisions, as well as common law doctrines like impossibility, illegality and frustration of purpose to excuse nonperformance. The Russian court practice that emerged after the Ukraine conflict generally treats sanctions as illegal or contradictory to public policy.

Complex conflict of laws situations, and public policy considerations, as well as contract governing law and dispute-resolution clauses, have played an important role in determining clients' contract or defense strategies.

As a result, companies with global operations should evaluate their contractual relationships and identify any agreements or counterparties that may be affected by sanctions.

They should anticipate that counterparties may invoke sanctions in an attempt to excuse their performance under contracts. They should also consider if and how these sanctions may impede their own performance. They should also review their contracts or model contracts to determine whether they need to be adjusted to address the global conflict's challenges.

Insurance

The scope of coverage afforded by first-party business insurance policies has come into sharp focus during the conflict. Typical commercial property insurance provides all-risk coverage for loss or damage to the insured's property. While coverage may be subject to an exclusion for loss caused by war, hostilities, confiscation, detention or nationalization, many policies contain endorsements extending coverage for such causes of loss.

Additional coverage available under commercial property insurance policies varies.

For instance, contingent business interruption coverage protects the insured from loss associated with supply chain disruptions caused, in whole or in part, by third-party property loss or damage. The property loss or damage must be caused by a peril covered under the policy.

While contingent business interruption coverage generally does not reach losses caused by war, political disruptions, road closures, or bankruptcy of a business partner or supplier, endorsements writing back the coverage exist.

Sub-limits are generally applicable to contingent business interruption or supply chain coverage, and may vary depending on property loss or damage suffered.

Other specialty coverages may be available to cover business or industry-specific risks, as with aviation, marine and cargo risks, either on standard or manuscripted forms.

It is important to carefully review for potential coverage, including applicable policy limits and sub-limits, coverage enhancements, exclusionary clauses, and interplay among all potentially applicable local and global policies.

Cybersecurity

Many companies look to increase their cyber defenses amid heightened geopolitical tensions as threats of ransomware and data breaches continue apace, particularly with respect to critical physical and digital infrastructure.

The risk of data breaches and their adverse impacts on businesses — from unwelcome publicity to brand damage — pose some of the greatest risks to modern companies.

In addition, legislators and regulators, especially in the U.S., EU, U.K. and Asia-Pacific region, are seeking to apply and enforce industry-specific cybersecurity laws — such as the EU's robust NIS 2 laws.

A ransomware attack is not a new phenomenon. But the dramatic uptick in these types of cyberattacks and the public's response could ignite a force majeure firestorm. In fact, as cyber criminals target critical infrastructure, companies need to think about the security of an individual entity as well as widespread disruption to the broader supply chain and economy.

Unfortunately, there is no one-size-fits-all solution.

However, a key preparedness strategy is to consider the cybersecurity risk profile of the company's manufacturing and services lifecycle — not just those relating to information systems.

Importantly, the company's board and its senior business and legal team — not just its information security team — should consider training regularly for a bet-the-company eventuality, including having to make difficult business and legal choices under pressure.

The conflict in Ukraine has raised significant cybersecurity concerns for global businesses, resulting in an increased use of cyber insurance to mitigate any resulting losses. It has also caused insurers to turn their attention to a rarely invoked exclusion in insurance policies: the war exclusion.

Certain insurers have recently taken steps toward altering the language of such exclusions. As a result, evaluating the applicability of insurance coverage, including the specific language of any war exclusions contained in the policies, is an important first step for businesses as they seek to protect themselves from cyber threats.

Online Content Moderation

States in conflict — and their supporters — increasingly seek to proliferate misinformation — including misinformation generated by artificial intelligence — on websites and online platforms and intermediaries. This creates strategic business, legal and reputational risks for all companies.

Companies may wish to proactively consider their exposure and implement appropriate business, communications and legal strategies in advance of any such risks being realized — e.g., creating a special team to respond promptly, submit appropriate take-down requests and implement defensive communication strategies.

In addition, many countries — notably, the EU via the Digital Services Act and the UK via the Online Safety Act — are enacting, or have enacted, laws requiring operators of certain websites, social platforms, hosting companies and other online intermediaries to implement policies and procedures for actively monitoring and removing certain user-generated content made available, hosted or transmitted

through their platforms.

However, obligations under these laws extend to many types of content — for example both unlawful content and lawful-but-awful content. This creates potential conflicts with other laws relating to freedom of expression, data protection and antitrust.

Companies failing to comply with these new content moderation laws may be exposed to potentially significant fines.

Employees

Addressing employee expression in the workplace becomes more complicated during times of conflict. Employers can regulate employee expression through personnel policies, but laws that protect political speech within or outside the workplace can require employers to limit the scope of those policies.

Moreover, in the social media age, a company seeking to avoid the fray may be compelled to respond to employees' public commentary, even when the employee makes those comments outside their company role.

If the employer is silent, some may construe that silence as an endorsement. If the employer disciplines the employee for expressing their views, divisions may occur among the workforce.

Discipline could also create employment law risks, such as claims of discrimination based on the employee's race or national origin.

In some circumstances, the employer may have no choice but to remain publicly silent if the employee's controversial commentary qualifies as protected activity under applicable laws.

Fortunately, many jurisdictions' laws contain exceptions that balance the employee's right to political expression with the employer's interest in maintaining a safe and respectful workplace.

Immigration

The Ukraine conflict has highlighted several dichotomies of global conflict in the immigration space. On the one hand, borders were opened to fleeing Ukrainian nationals through refugee and asylum streams. These streams provided residence and work permissions in countries around the world.

On the other hand, there were no accommodations made for Russian nationals, and companies looking to move employees out of harm's way encountered roadblocks as embassies and consulates banned, deprioritized or applied more scrutiny to the entry of Russian nationals.

Additionally, when the military reserve was mobilized in Russia, global mobility teams coordinated with the local experts to evaluate the local civil and criminal laws for companies and individuals associated with the draft.

Conclusion

When new global conflicts arise or, as in the case of Ukraine and Russia, existing conflicts continue for several years, the lessons of the past outlined here may help protect the future of global commerce.

David Plotinsky is a partner at Morgan Lewis & Bockius LLP. He formerly served as acting chief of the U.S. Department of Justice's Foreign Investment Review Section.

Vasilisa Strizh is a partner at Morgan Lewis.

Vishnu Shankar is a partner at Morgan Lewis.

Morgan Lewis partners Shannon Donnelly, Daryl Landy, Paul Mesquitta, Sergio Oehninger and Peter Sharp contributed to this article.