The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Companies Want To Avoid Liability for War-Related Damages. That Might Be Impossible.

By Sarkis Darbinyan

November 04, 2026

Smoke billows from a Wildberries warehouse in Elektrostal, Moscow region. **Social Media / via REUTERS**

Customers of Beget, one of Russia's largest hosting providers, have received an "official notification of force majeure circumstances" after a massive cyberattack has crippled the company's infrastructure: its name servers and email services are down and some customers' data is being restored from backups. No one has given a timeline for when normal operations will resume.

Beget cites Article 401, Paragraph 3 of the Russian Civil Code, stating that the attack is temporarily preventing it from fulfilling its contractual obligations.

A hosting provider declaring a cyberattack to be force majeure is like a fire department refusing to put out a fire because there is a fire. Protecting servers against attacks is precisely

what customers pay hosting providers to do.

But there is little reason to be surprised by this. Beget is simply following a path already well worn by larger companies over the past few months.

Wildberries was first. A clause appeared in the July 7, 2026, version of its terms of service defining force majeure to include "any consequences of the use, impact, fall, launch or activation of weapons, including unmanned aerial vehicles."

Shortly afterward, a Wildberries warehouse in Elektrostal burned down, with goods belonging to numerous sellers going up in smoke. Wildberries owner Tatyana Kim promised installment payment plans, loan repayment holidays and support, but the company's lawyers warned that the marketplace had no obligation to compensate sellers for their lost goods. The cause of the fire was never officially disclosed.

On October 8 and 9, drones struck Yandex data centers in Sasovo and Kaluga. The next day, a force majeure section appeared in Yandex's user agreement that had not been present in its 2025 version. The “clarifications” — in the company’s words — covered military operations and terrorist attacks, including those involving drones and missiles, mandatory evacuations, and accidents affecting energy and communications infrastructure.

Now comes Beget. I would wager that within six months, a similar clause will appear in the terms of service of every company operating a server or warehouse, or purchasing any kind of IT service, within range of Ukrainian drones.

Here’s what the law says. The Russian legal code takes a strict approach to force majeure. A business is liable for breaching a contract even when it is not at fault and is exempt from liability only if it proves that performance became impossible because of extraordinary and unavoidable circumstances.

In 2016, the Plenum of the Supreme Court explained how this should be assessed in Paragraph 8 of Resolution No. 7. A circumstance is considered unavoidable if no other business engaged in the same activity could have prevented it. The benchmark is a reasonably competent professional with a security budget typical of the industry, not a particular company that has economized on protection.

Such questions must always be assessed on a case-by-case basis. In spring 2020, the Supreme Court explicitly stated that the pandemic could not automatically be treated as force majeure in every situation. Similar disputes arose over sanctions in 2022, which the courts likewise refused to recognize automatically as force majeure.

Case law concerning drone strikes is only beginning to emerge, with the decisions so far being inconsistent. In June, the Moscow Arbitration Court accepted that a drone attack could constitute force majeure, depending on the circumstances. In May, however, the Moscow Region Arbitration Court rejected a supplier's attempt to invoke a drone strike against one of its customers. Neither decision has yet entered into legal force.

Related article: Yandex Suspends 2026 Guidance After Data Centers Come Under Fire

All three companies — Wildberries, Yandex and Beget — face the same problem. Extraordinary circumstances are supposed to be unexpected.

It isn't clear that drone attacks fulfil this criterion. Oil refineries have been under attack for several years. Since the beginning of October, three Yandex data centers have been attacked, as have data centers belonging to Sberbank and VKontakte.

In August, Putin signed Decree No. 604, allowing critical infrastructure facilities to be placed under temporary state administration if they are inadequately protected, including against drones.

More recently, Decree No. 802 was issued requiring private data centers to reserve 10% of their capacity for the state. The justification is explicitly stated: "unfriendly actions by certain foreign states."

When the state regards attacks as so predictable that it requires companies to prepare for them and punishes failures to do so, it becomes difficult to convince a court that another strike came as a complete surprise to a warehouse or data center operator.

Furthermore, the fact that Wildberries and Yandex explicitly included drones in their contracts is further proof that they anticipated this risk. You cannot simultaneously tell a court that an event was unforeseeable and produce a contract in which you foresaw it.

There is a separate irony here. Officially, Russia is not at war, nor is it under martial law or a state of emergency. Officially, the invasion is still a "special military operation," and using the word "war" can still land you in prison.

Yet the terms of service of Russia's largest companies already refer to "military operations." Corporate lawyers are calling things by their proper names before anyone else is allowed to. Or perhaps this is a clever corporate maneuver: neither a war nor an operation, just military activity.

Related article: Russian Courts Paralyzed by Yandex Cloud Outages After Drone Attacks – Vyorstka

Companies will argue that parties are entitled to decide for themselves what constitutes force majeure in their contracts, and that courts generally respect such agreements. That is true, but there are three caveats.

First, contracts cannot be rewritten retroactively. Yandex added drone strikes to its agreement two days after the attack on its Sasovo facility. The new terms do not apply to obligations breached before October 10 and unilateral changes to contractual terms are prohibited altogether for individual consumers.

Second, certain legal provisions cannot be circumvented by contracts. Wildberries charges sellers to store their goods in its warehouses, making it a professional custodian. Back in 2012, the Presidium of the Supreme Arbitration Court, ruling on a warehouse fire case, held that a professional custodian's liability for the loss of stored property cannot be reduced by contractual terms.

Third, the terms of service of a marketplace or hosting provider constitute an adhesion contract. Customers can only accept the company's terms, not negotiate them. Under Article 428 of the Civil Code, the party accepting such a contract, including a business, can demand that it be amended or terminated if it excludes or limits the stronger party's liability and contains manifestly burdensome provisions. Wildberries' liability cap of 0.1% of the cost of its services fits that description rather well.

Related article: From Wildberries to Yandex, Ukraine Is Turning Russian Business Giants' Dominance Into a Liability

Beget has the weakest position of the three companies. As a hosting provider, a cyberattack is an ordinary professional risk. DDoS protection, network segmentation and backups stored in an isolated environment are integral parts of the service.

Beget says that file backups are available for the "overwhelming majority" of its customers' resources, meaning that not everyone is covered. This raises questions about the company's infrastructure design, not the identity of its adversary.

To establish that the attack constituted force majeure, Beget will have to prove that any hosting provider of comparable size, equipped with reasonable protections, would have suffered exactly the same fate.

Allegations that Ukrainian state-backed hackers were responsible are unlikely to help establish attribution in an arbitration court.

Beget has provided little detailed explanation of what kind of massive attack it suffered or which attack vectors were used.

But Beget's customers should now be thinking about something else. If their websites contained personal data and they cannot rule out the possibility that someone gained unauthorized access to it, they themselves, as data controllers, are obliged to notify Roskomnadzor within 24 hours.

Turnover-based fines for data breaches are already in force, and citing a hosting provider's force majeure declaration will not provide a defense. Some stolen data may be lost forever.

Traditionally, no one wants to assume the risks of war in commercial transactions. Article 964 of the Civil Code exempts insurers from paying compensation for damage caused by military operations unless the insurance contract provides otherwise.

The state compensates businesses for damage caused by attacks selectively and at its own discretion.

Large platforms are therefore filling this gap in the only way available to them: shifting the risk onto those who lack the bargaining power to resist, whether marketplace sellers or hosting customers.

Civil law rests on a simple principle: risk is borne by whoever controls an operation and profits from it. Wildberries controls its warehouses, Yandex controls its data centers, and

Beget controls its servers.

War puts this logic to the test. If courts begin recognizing anything even remotely connected to the war as force majeure, the Civil Code will effectively be rewritten without any involvement from the State Duma, simply through the terms of service imposed by major companies.

Sellers will pay warehouses to store their goods without the warehouses bearing responsibility for keeping them safe. Customers will pay for hosting services whose providers bear no responsibility for keeping their websites online.

Meanwhile, the rules of the market are also being rewritten from above, through presidential decrees.

As mentioned earlier, Putin has ordered private data center owners to reserve 10% of their space and capacity within 10 days. At the direction of a new subcommission under the government's commission on digital development, they must make this reserve available within 24 hours to support the functioning of information resources at a government-determined price.

Since August, operators that inadequately protect their facilities can be placed under temporary state administration without a court order. The same decree also generously permits Russian information resources to be temporarily hosted in foreign data centers. That decision rests with the same government subcommission, but requires approval from the FSB.

After all, you cannot simply install the systems required under the Yarovaya laws or SORM surveillance equipment in those facilities. That means falling back on the old-fashioned approach: submitting a detailed written report and being ready to hand over data at any moment.

Related article: Is Washington Getting Special Treatment as Putin Goes After Western Companies?

For those affected by the Beget cyberattack, my advice would be to not accept a force majeure notification as the final word. Document your losses, preserve every communication from the company, find the version of its terms of service that was in force when the incident occurred and demand evidence from the company.

Anyone can declare force majeure. Proving it in court is another matter.

The question is whether Russian courts in 2026 will be willing to protect the weaker party to a contract when it is up against major, systemically important companies such as Wildberries, Yandex and Beget.

And are they even prepared to acknowledge any consequences of a war that officially does not exist?

Recognizing a drone strike as force majeure would mean stating in a court ruling that the country is in its fifth year of war. It would mean ordering a company to pay compensation for

losses caused by the state's own war.

In any case, force majeure exempts a party from liability only for as long as the circumstances persist. There is only one way to bring this to an end: end the war.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2026/11/04/russian-companies-want-to-avoid-liability-for-war-related-damages-that-might-be-impossible-a94178