



By: TA Analysis

Russian digital economy within range of Ukrainian drones



Russian technology giant Yandex announced that operations at its data-processing centre in Vladimir had been completely suspended after a drone strike.

The company described the **remaining infrastructure** as unstable, warned that technical support could also be interrupted and urged customers to activate alternative business continuity plans.

This was the third major Yandex facility hit in four days, following the shutdown of the centre in Sasovo on 8 October and damage to equipment in Kaluga the following morning.

The extent of the damage and the timeframe for recovery have not yet been determined.

On 8 October, Ukrainian President **Volodymyr Zelenskyy**, responding to a question about the first attack, said that Ukraine was retaliating against Russian attacks on its data-processing centres. 'We always respond in kind,' he told reporters, adding that he could not provide specifics.

The **statement** came ahead of talks between the Ukrainian delegation and US negotiators in Miami on 9 and 10 October, at a time when it was already clear that large commercial data centres were also directly exposed to the war.

Moscow's long-standing requirement that Russian citizens' data be processed in domestic facilities is now making it difficult for companies to relocate quickly from damaged centres.

Other Russian services are also facing a shortage of available capacity, as large numbers of users simultaneously look for new locations.

Ukraine's explanation for the strike raises a separate legal issue that can be resolved only with evidence that the affected facilities actually served military operations.

How mandatory data storage makes recovery difficult

Since 2015, Russia has required that the **personal data** of its citizens be collected and processed in databases located on its territory.

Amendments taking effect in July 2025 further tighten restrictions on the use of foreign databases for the collection, storage and updating of such data.

At the same time, the Russian Ministry of Digital Development has confirmed that the law allows the subsequent transfer of data to other countries, subject to prescribed conditions.

The regulation therefore does not prohibit all transfers of data abroad, but it does prevent a company from simply cancelling its obligation to maintain a domestic database by moving to a foreign server.

Yandex Cloud, Yandex's server and data-space rental service, operates across four data centres in Russia.

All four form a single unit, so when one fails, clients are transferred to the remaining centres.

Clients can look for other Russian providers, but large numbers of companies are trying to do the same at the same time

After the attack on Vladimir, the company warned that the remaining capacity was operating in emergency mode.

Yandex also has a separate centre in Kazakhstan, but the data of Russian clients is not stored there, so the company cannot simply continue working from Kazakhstan when a Russian centre shuts down.

It would have to transfer the data itself, which requires time, spare capacity and compliance with Russian data-protection law.

Clients can therefore look for other Russian providers, but large numbers of companies are trying to do the same at the same time.

For some business applications, changing provider also means adapting the software to a new system, so even spare capacity in another centre does not guarantee a rapid resumption of work.

Amazon found itself in a similar situation in March this year, during the war with Iran.

Two of its data centres in the **United Arab Emirates** were hit by Iranian drones, and a third, in Bahrain, was damaged when a drone crashed nearby.

Amazon advised customers to move their systems to its centres in other parts of the world, and many firms did so.

Yandex clients do not have that option. Russian law requires the data of Russian citizens to remain in Russia, and almost all of Yandex's centres are in the central part of the country, several hundred kilometres from Moscow and within range of Ukrainian drones.

When several centres were hit in quick succession, clients had nowhere to go.

Why a saved copy is not enough

In the first six months of this year, **Yandex Cloud** had about 64,000 business clients and revenue of 16.7 billion roubles, approximately \$200 million, 30 per cent more than a year earlier. Most of its users are banks and other financial firms, traders and IT companies.

At Yandex, they rent servers on which they host their applications, receive orders and process the data they need every day for their work.

When the server stops, so does their business. The owner of **Pulse**, a small Russian dating app with about 8,000 users, told reporters that after the first attack he could not even obtain a backup copy of his data. He did not know whether the data was lost, but the app was already down.

Yandex agreed with three Russian competitors to take on its affected customers

Saved data does not restore operations immediately either. The company must first find available servers in another centre, restart its programmes there and check that everything is working as it should.

Yandex therefore agreed with three **Russian competitors** – Selectel, K2Cloud and VK Cloud – to take on its affected customers. Companies from other Russian cities were left without their applications and data because they kept them on Yandex's servers in Sasovo, a town about 350 kilometres south-east of Moscow.

When the drone hit that centre, their business also stopped, even though their offices and computers were not affected.

Uncertain fate of three Yandex supercomputers

In November 2021, Yandex announced that its three most powerful supercomputers were located in the very centres that were attacked this week.

The supercomputers Chervonenkis and Lyapunov were in Sasovo, and Galushkin was in Vladimir. Yandex develops its artificial intelligence on such machines.

The three systems had 3,776 Nvidia graphics processors which Russia can now hardly buy or replace due to Western sanctions

Together, the three systems had 3,776 **Nvidia graphics processors**, specialised chips for the most demanding calculations, which Russia can now hardly buy or replace due to Western sanctions.

Yandex did not say whether those computers

are still in the same locations today or whether they were damaged.

If they were, Russia has lost part of the strongest computing power for the development of artificial intelligence at its disposal, which it will not be able to replace quickly under sanctions.

The military significance of the objective must be established

Russia started this war and has systematically targeted Ukrainian infrastructure for years.

According to the UN human rights office, from October 2025 to March 2026 it carried out at least 423 attacks on power plants and transmission lines and at least 74 on heating plants.

Households, hospitals and schools were left without electricity for days, and hundreds of thousands of people were left without heating in the midst of extreme cold.

From December to May, 1,272 civilians were killed in Ukraine and 6,871 were wounded.

Russian attacks on data-processing centres and internet providers in Kyiv left about 100,000 households without internet

At the end of September, **Russian attacks** on data-processing centres and internet providers in Kyiv left about 100,000 households without internet. Moscow claimed that these centres worked for the Ukrainian army but provided no evidence.

Zelenskyy presented the attacks on Yandex centres as a response to those strikes.

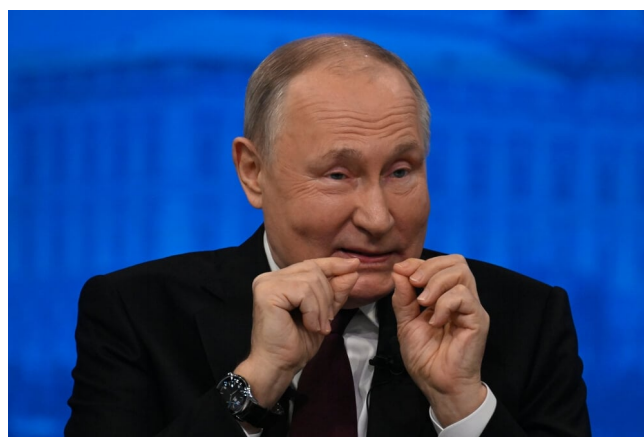
The law of war, accepted by both Russia and Ukraine, prohibits **targeting civilian objects** in retaliation, even when an adversary has done so first.

A data-processing centre becomes a legitimate target if it is used for military operations, and even then the attacker must ensure that the harm to civilians is not disproportionate to the military advantage. Kyiv has not yet said whether Yandex's centres served the Russian military.

The possibility of state management

The Kremlin already has a legal basis for such a situation. On 24 August, Putin signed a decree allowing the state temporarily to take over the management of important infrastructure facilities if their owners do not protect them from attacks or fail to restore them afterwards.

The administration would then be taken over by the Federal Agency for State Property Management, Rosimushchestvo, or by a manager appointed by the government.



Putin signed a decree allowing the state temporarily to take over the management of important infrastructure facilities if their owners do not protect them from attacks

No such action has been taken against Yandex, but the company now admits that it does not know when it will repair its centres.

Yandex has been Russian-owned since 2024, when its Dutch parent company sold its Russian business to a group of Russian investors, and the Kremlin at the time described it as the nation's tech champion.

Meanwhile, the company is protecting itself

from its customers. On 10 October, Yandex added a provision to its terms of service stating that military operations and drone strikes are considered force majeure, which can exempt it from liability for outages.

It claims it was merely standardising rules that already existed, but companies left without their systems must now check their contracts to see whether they can claim damages.

Recovery over the coming weeks will depend on how many spare servers other Russian providers have and how quickly Yandex can acquire new equipment under sanctions.

The longer the outages last, the more grounds the state will have to dictate how private companies must protect their centres and to check that they are doing so.

For years, the Kremlin has forced companies to keep the data of Russian citizens in Russia. Now it has a decree that, citing Ukrainian drones, also allows it to take over the management of the centres where that data is stored.