

Data centres in Russia: the consequences of Ukrainian drone strikes

Iwona Wiśniewska

Between 7 and 11 October, Ukrainian drones struck three data centres belonging to the Russian technology company Yandex. On 14 October, another data centre in Balakovo (Saratov Oblast), owned by Sberbank – Russia’s largest commercial bank – came under attack. On 18 October, a server facility in Leningrad Oblast used by VK (formerly VKontakte, Russian: ВКонтакте), the country’s largest social network, was also hit. Both Sberbank and VK confirmed strikes on their facilities, while maintaining that their systems continued to operate without disruption. Yandex, however, acknowledged that operations at two of its affected data centres – in Sasovo (Ryazan Oblast) and Vladimir – had been completely suspended, while infrastructure at a third facility in Kaluga had been hit. The attacks also damaged their power supply systems. Consequently, the company has been operating in emergency mode since 8 October. The strikes have caused serious disruption to Yandex’s online services, including its most popular offerings: its search engine, and transport, navigation and payment services. However, the consequences extend much further. Around 64,000 customers used Yandex Cloud services, including major companies in the financial, retail and IT sectors. The attacks may also have damaged Russia’s three largest supercomputers, housed at the affected facilities and used for a range of purposes, including the development of Russian artificial intelligence models.

It is worth noting that Russian forces have been conducting large-scale attacks on data centres in Ukraine since mid-September. On 27 September, in one of the most serious attacks, 10 data centres in Kyiv and one in Dnipro were damaged, including server facilities operated by telecommunications providers Kyivstar and Ukrtelecom. On 10 October, Russian drones also damaged a technology facility in Odesa belonging to the operator TENET.

Data centres are the latest category of targets struck by the Armed Forces of Ukraine deep inside Russia, following oil industry facilities and e-commerce platforms. Although the consequences of these attacks are not critical to the Russian economy, they will exacerbate the country’s existing economic problems, adding to inflationary pressures and adversely affecting budget revenues. The damage caused by the drones also directly undermines the interests of the Putinist elite, whose members control virtually all profitable corporations in Russia, including Yandex and VK. Moreover, the attacks have an important psychological dimension, as they make Russian society increasingly aware of the cost it is paying for the country’s involvement in the war. One of the objectives of the Ukrainian campaign is to fuel tensions both within the elite and across society.

Commentary

- **So far, attacks on data centres have had a limited impact on the functioning of the Russian economy.** Three of Yandex's six data centres have been affected (although two separate facilities are located next to each other in Vladimir, and it remains unclear whether only one was damaged). In Sberbank's case, one of the three data centres supporting its infrastructure was hit. Russia has approximately 200 large data centres of this type, the vast majority of which (over 80%) are located in Moscow and St Petersburg, the cities with the strongest air defences.
- **The main obstacle to the functioning of Russia's technology sector is the Kremlin's *policy of establishing a sovereign Russian internet*.** Among other measures, the Kremlin has forced Russian technology companies to store all their data on domestic servers, preventing them from storing backup copies beyond the reach of drones and missiles. By contrast, Ukrainian companies have maintained their operations despite large-scale Russian attacks on data centres in Ukraine by using servers and cloud infrastructure in the European Union. Moreover, Russian servers are under strain from the volume of data that domestic entities are required to retain, officially for internal security purposes but in practice also for surveillance and social control (for example, users' voice messages, text messages and images must be stored for three years). They are further burdened by the extensive hardware and software installed across the network to monitor the population. Consequently, the loss of even a small proportion of computing capacity due to drone strikes disrupts the functioning of the entire system, while some services may become completely unavailable because they rely on a single data centre.
- **The losses caused by damage to data centres could prove greater than those resulting from attacks on e-commerce platforms.** Yandex has a near-monopoly in the market for commercial technology services (not only in Russia but also in Belarus, Central Asian countries and Serbia), particularly in ride-hailing and navigation services. Disruptions to these services forced the company to issue a statement encouraging users to switch to alternative services, such as Google Maps. Restoring the system to full functionality will require substantial investment and time, with estimates suggesting that it will take at least six months.
- **Russia remains entirely dependent on imports of the IT hardware needed to operate data centres.** However, given the rapid growth of this industry worldwide, finding a supplier at short notice is difficult. Moreover, sanctions force Russian companies importing advanced technologies to rely on multiple intermediaries and pay them substantial fees to compensate for the risks associated with facilitating sanctions circumvention.
- **Attacks on data centres are worsening Russia's technological decline, which has continued since the start of the full-scale war.** The main causes are underinvestment, stemming from limited financial resources, and the loss of access to Western technologies. Over more than four years of war, Yandex has strengthened its position in the domestic market owing to a lack of competition, but has fallen further behind global industry leaders. In 2021, five Russian supercomputers were among the world's 100 most powerful machines in the TOP500 ranking. The most powerful of these (located in Sasovo and owned by Yandex) ranked 19th at the time, but had fallen to 101st by June

2026. Moreover, no new supercomputers have become operational in Russia since 2021. The most advanced project was Sberbank's largest supercomputer, under construction at the recently attacked data centre in Balakovo. Construction began in 2020, with commissioning scheduled for 2027. Significantly, all Russian supercomputers were built using hardware supplied by the US company NVIDIA. If reports that these machines were damaged in the attacks are confirmed, as suggested by widespread problems reported by users of the AI-powered virtual voice assistant Alisa, Russia will fall even further behind the world's technological leaders.