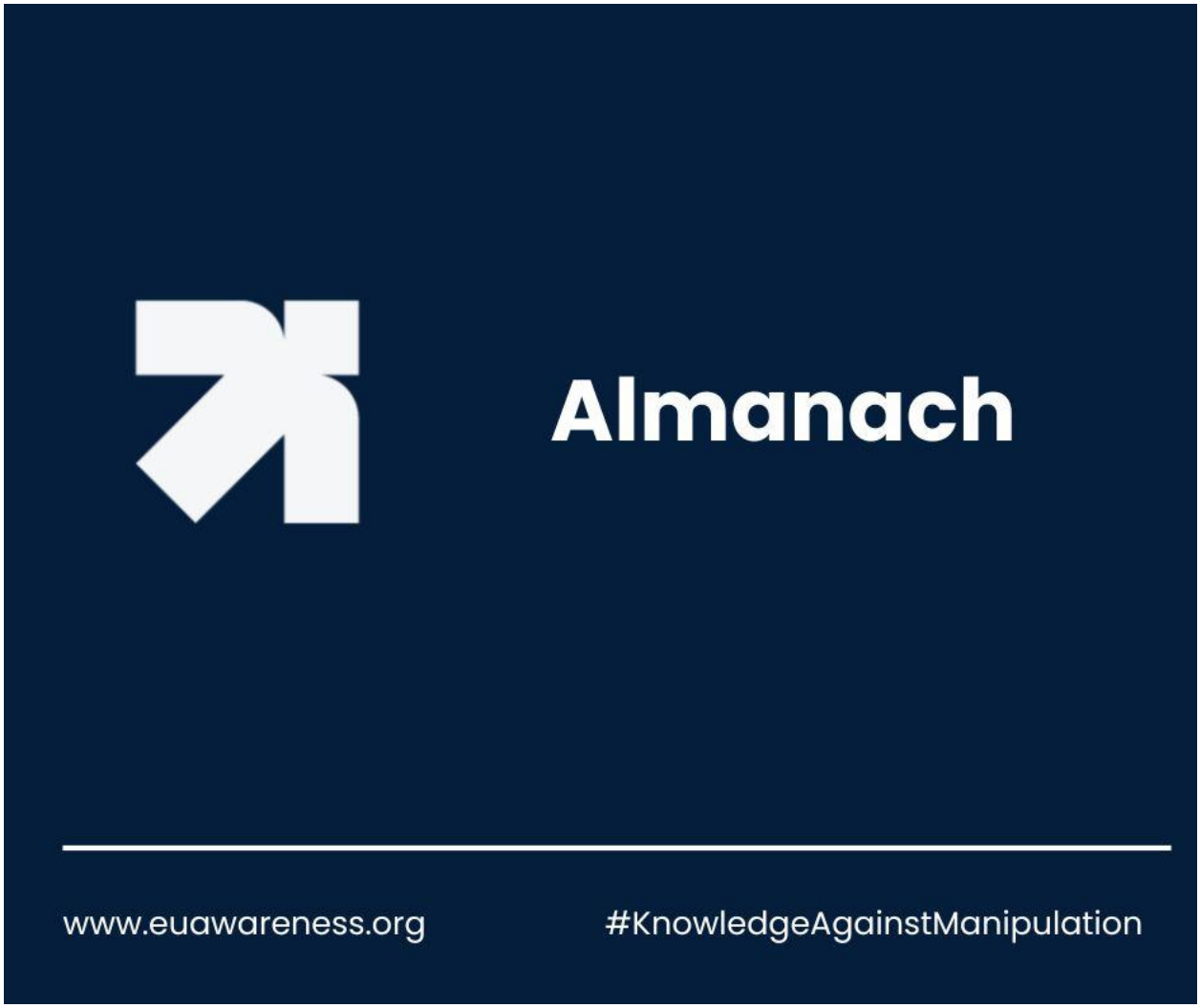


Almanach #18

Diana Sviderska

Beyond the Bots: What the Attack on Russian Data Centres Reveals About Foreign Influence Operations

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

© [2026] EU Awareness Centre. All rights reserved

12 November 2026

Beyond the Bots: What the Attack on Russian Data Centres Reveals About Foreign Influence Operations

This commentary examines the scale and mechanisms of Russian online influence operations in the context of Ukraine's strikes on Russian Yandex data centres and the subsequent claims of declining bot activity. It questions whether disruptions to digital infrastructure can significantly weaken foreign influence and explores why such assumptions may oversimplify the problem. Moving beyond automated accounts, the commentary considers how Russian-aligned actors exploit existing social and political divisions to undermine public trust and democratic resilience. It concludes by identifying lessons for democratic societies on how to respond to these threats.

Recently, news about Ukraine's strikes on Russian data centres was accompanied by claims that the attacks had caused a decline in Russian bot activity online. Some users connected these developments to reduced online activity surrounding the far-right Alternative for Germany (AfD) in Germany and accounts supporting Donald Trump in the United States. Although no verified evidence established a direct connection between the strikes and these reported changes, the discussion raised a broader question about the scale of Russian influence online and why so many people were quick to believe that a Ukrainian strike could significantly weaken it.

The Ukrainian attacks disrupted more than 80 services and cloud infrastructure components. Yandex confirmed that operations at its Vladimir facility had been halted. The affected systems included cloud computing, storage, databases, and artificial intelligence tools, along with consumer products such as the Alice voice assistant, Yandex Music, and videoconferencing services.

After the attacks, President Volodymyr Zelenskyy commented that social media had become less hostile, while online users reported a decline in bot activity. As Euronews reported, these claims were also connected to reports of reduced online activity surrounding the AfD in Germany.

Czech MEP Tomáš Zdechovský questioned the apparent coincidence between the disruption and the reported decline in activity around the party:

"If confirmed, this is telling: Russian data centres get hit, and online activity around AfD suddenly plummets," he wrote on X.

Similar claims emerged in Britain, where online activity associated with Reform UK was also reported to have declined following the attacks, as former US Ambassador Michael McFaul pointed out on X.

However, other assessments questioned whether the disruption had any demonstrable effect on Russian influence operations. Roman Osadchuk, Director of Threat Intelligence at the technology company LetsData, explained to the Kyiv Independent:

"No reliable graph can consolidate bot and troll activity across multiple social media platforms without their internal data that measures telemetry, traffic, and behaviour."

A troll farm, or troll factory, is an organised group involved in coordinated online influence operations. Its activities are not necessarily limited to automated accounts or fake profiles. A 2017 investigation by The Guardian, for example, reported that a Russian troll factory had paid US activists to help fund protests during the election period. This illustrates how such operations can extend beyond automated online activity and involve real individuals.

Nevertheless, these mechanisms represent only part of a much broader picture. Not all influence operations rely on spreading false information. Many aim to undermine public trust, deepen social divisions and delegitimise democratic processes and institutions.

They can do this not only by creating false narratives but also by exploiting existing disagreements within communities. Relations between Poland and Ukraine, immigration debates across Europe and political divisions in the United States are examples of complex issues that can become targets for foreign influence. Rather than inventing entirely new problems, Russian-aligned actors can amplify existing tensions by circulating increasingly radical opinions and presenting them as widely shared public sentiment.

The relationship between Poland and Ukraine illustrates this dynamic. Despite Poland's significant support for Ukraine, tensions between the two societies have emerged around a range of political, economic and historical issues. At the same time, Ukrainian refugees have contributed substantially to the Polish economy.

According to a UNHCR–Deloitte analysis, refugees from Ukraine contributed 2.4% of Poland's GDP in 2025. These disagreements are real and cannot be dismissed as propaganda. However, external actors can also exploit them to deepen divisions.

An investigation by the Institute for Strategic Dialogue found that Russia-aligned campaigns amplified negative sentiment towards Ukrainians in Poland ahead of the 2025 presidential election. These campaigns used fabricated stories and coordinated online activity to intensify anti-Ukrainian sentiment and exploit existing social divisions.

The danger lies in creating the impression that extreme positions represent the views of a much larger part of society than they actually do. Narratives that might otherwise remain on the margins can be amplified until they appear to reflect widespread public opinion. This can make constructive discussion more difficult and contribute to real-world tensions between communities and countries.

Therefore, treating every disagreement as foreign propaganda would be just as misleading as ignoring the role of foreign influence altogether. The existence of Russian influence operations does not mean that the underlying social and political problems are imaginary. Rather, it demonstrates how genuine concerns can be manipulated and intensified for political purposes.

This also helps explain why the idea that Ukrainian strikes on data centres could simply free Western online spaces from Russian influence is so appealing. There is a temptation to look for a straightforward technical solution to a complex political problem, rather than acknowledge how deeply information operations can penetrate society. Disrupting digital infrastructure may affect the services hosted there, but it does not automatically eliminate the networks, narratives and social conditions that allow influence operations to continue.

The incident therefore raises a broader question: how dependent are influence operations on digital infrastructure, and how resilient are the societies they target? Russia has invested considerable resources in its information technology capabilities, using digital platforms and infrastructure not only to shape the information environment within its own borders but also to influence political and social developments abroad.

Disinformation is often understood as the deliberate spread of false information. Governments have traditionally attempted to address it by identifying, removing or debunking false narratives on the platforms where they circulate. However, the Yandex incident demonstrates why this approach alone is insufficient.

Democratic states need to look beyond individual false narratives and strengthen their resilience to foreign influence. This requires greater transparency and accountability from online platforms, as well as meaningful access to platform data for independent researchers. As Roman Osadchuk noted in an interview with the Kyiv Independent, reliably assessing bot and troll activity across multiple social media platforms requires access to platforms' internal data. The EU Digital Services Act provides a framework for improving platform transparency and enabling vetted researchers to examine systemic risks. Strengthening media literacy and public awareness is equally important, helping societies recognise manipulation and respond critically to misleading information.

Ultimately, the attacks on Russian data centres may have disrupted important digital services, but they should not be mistaken for a solution to the wider problem of foreign influence. Disrupting infrastructure does not necessarily eliminate the networks, strategies or audiences that sustain information operations. The challenge for democratic states is therefore not simply to disrupt the infrastructure behind online activity, but to understand how influence operations function, how they reach audiences and how societies can become more resilient to them.



Diana Sviderska is a student of the International, European and Comparative Legal Studies (IECoLS) bachelor's programme at the University of Macerata, Italy. Her academic and professional interests focus on international law, advocacy and European integration, particularly in the context of Ukraine–EU relations