

Russia is responsible for destructive and disruptive cyber-attacks against Denmark

December 18th 2025

The Danish Defence Intelligence Service (DDIS) assesses that Russia was behind a destructive cyber-attack on a Danish water utility in 2024 and a series of DDoS attacks on Danish websites in the run-up to the 2025 municipal and regional council elections.

The DDIS assesses that the pro-Russian group Z-Pentest, which carried out the destructive attack on the water utility in 2024, has links to the Russian state. Also, the DDIS assesses that the group NoName057(16), which carried out DDoS attacks on Danish websites ahead of the 2025 municipal and regional elections, has links to the Russian state.

The Russian state uses both groups as instruments of its hybrid war against the West. The aim is to create insecurity in the targeted countries and to punish those that support Ukraine.

Russia's cyber operations form part of a broader influence campaign intended to undermine Western support for Ukraine. The DDIS assesses that the Danish elections were used as a platform to attract public attention – a pattern that has been observed in several other European elections.