

Question for written answer E-003871/2025
to the Commission
Rule 144
Dan-Ştefan Motreanu (PPE)

Subject: Cybersecurity: Rising foreign-sponsored attacks threaten EU security

In its latest annual report, the European Union Agency for Cybersecurity (ENISA) warns of a sharp increase in cyberattacks targeting EU Member States, with a growing share originating from foreign networks. ENISA analysed nearly 4 900 incidents, noting that the threat environment is becoming more complex, with faster exploitation of vulnerabilities and increasingly sophisticated adversaries.

The five most affected sectors are public administration, transport, digital infrastructure and services, finance and manufacturing – together accounting for more than half of all reported incidents. Phishing remains the most common entry point, while distributed denial of service attacks and ransomware continue to disrupt operations. Alarming, almost 80 % of incidents are ideologically driven, with surges recorded during elections and geopolitical crises. Attacks on mobile devices are also rising due to outdated systems and poor update practices.

State-aligned proxies from Russia, China and North Korea feature prominently, with most Member States reporting at least one attempted intrusion linked to such networks. Poland, Germany and France have been the primary targets of Russian networks, while Chinese groups focus on Italy. Romania also recently reported major hybrid attacks during its elections, underlining the vulnerability of democratic processes to foreign interference.

In the light of ENISA's findings, what new measures will the Commission introduce to strengthen the EU's cyber resilience, protect critical infrastructure and counter state-sponsored interference?

Submitted: 2.10.2025