

**Question for written answer E-003554/2026
to the Commission**
Rule 144
Andi Cristea (S&D)

Subject: Autonomous AI-enabled cyberattacks and the protection of European critical infrastructure

In July 2026, during security evaluations of advanced AI models, several models reportedly bypassed safeguards intended to isolate them from the internet, gained external network access and compromised third-party infrastructure. They allegedly exploited vulnerabilities, obtained credentials without authorisation and accessed external systems without explicit instruction, in what was subsequently described as an unprecedented cyber incident.

This raises serious concerns about the ability of increasingly capable AI systems to autonomously engage in harmful cyber activities beyond controlled testing environments, posing risks to critical infrastructure and essential services, particularly in Member States such as Romania, which faces heightened cyber and hybrid threats on the EU's eastern flank.

In this context:

1. Does the Commission consider that the existing EU framework, consisting of the Artificial Intelligence Act¹, NIS 2 Directive² and Cyber Resilience Act³, adequately ensures the mandatory reporting and investigation of incidents involving advanced AI systems autonomously bypassing safeguards and compromising third-party systems?
2. Will the Commission, together with the European Union Agency for Cybersecurity (ENISA) and national authorities, assess EU preparedness for autonomous AI-enabled cyberattacks, including attacks in Romania and other eastern-flank Member States?
3. Does the Commission consider additional safeguards necessary, including mandatory independent safety and security testing, stronger controls on external network access during evaluations and mandatory reporting of serious AI-related security incidents?

Submitted: 8.9.2026

¹ Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).

² Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (OJ L 333, 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

³ Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (OJ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).