

(English version)

**Question for written answer E-002526/26
to the Commission
José Cepeda (S&D)
(17 June 2026)**

Subject: European cyber-army

Lithuania is facing a wave of cybersecurity threats from increasingly sophisticated, coordinated and aggressive agentic-AI-powered actors. These attacks are not an isolated case.

Europe is on the backfoot in terms of cybersecurity. We do not have our own CERN (Computer Emergency Response Network) to tackle AI military offensives. The EU does not have a singular intelligence system that protects Europe's comprehensive security. However, the alleged perpetrators of these cyberattacks do have an operational system where each cyberattack is coordinated with military operations, under the command of a singular military or intelligence organisation (GRU).

This — coupled with the new development of quantum computing and in conjunction with new offensive artificial intelligence (Mythos de Anthropic, OpenAI, China and its own developments, and Russia and its own developments) — amplifies these threats and leaves the EU in a very worrying situation.

1. What is the Commission's response to these threats?
2. Is the Commission planning to create an EU cybersecurity command centre as the basis for a future European cyber-army, acting as a single point of coordination operating with a singular European intelligence system?

Submitted: 17.6.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(10 September 2026)**

The EU Action Plan on Cybersecurity and AI⁽¹⁾ addresses risks and opportunities for cybersecurity posed by frontier AI models. It reinforces cybersecurity by promoting the implementation of relevant legislation, including Directive (EU) 2022/2555⁽²⁾, the Cyber Resilience Act⁽³⁾ and the AI Act⁽⁴⁾. It also outlines actions to upgrade existing vulnerability-handling processes for the age of AI-assisted vulnerability discovery.

Structured information sharing on AI-driven threats through existing networks such as the Computer Security Incident Response Teams Network is also essential.

Moreover, the proposed Cybersecurity Act 2⁽⁵⁾ will equip the EU Agency for Cybersecurity and the Commission with the resources and clarity of mandate that the new threat picture requires.

EU instruments, notably the European Defence Fund⁽⁶⁾ and the European Defence Industry Programme⁽⁷⁾, help Member States develop cyber capabilities to respond to AI-enabled threats in defence-critical environments.

The EU Cyber Blueprint⁽⁸⁾ sets a common framework to prepare for and respond to large-scale cyber incidents and crises. It integrates cyber crisis response with the EU's wider resilience, hybrid threat and civil-military frameworks, and reinforces cooperation with international partners, notably NATO. Further, the EU Cybersecurity Reserve supports Member States in responding to significant or large-scale cyber incidents.

The EU is strengthening its cyber defence posture in line with the EU Policy on Cyber Defence⁽⁹⁾ and Council Conclusions on the EU Policy on Cyber Defence⁽¹⁰⁾.

The EU Cyber Defence Coordination Centre aims to enhance coordination and situational awareness across EU and Member State cyber defence actors. An initial temporary nucleus of this EU capability has been in place as of July 2026, hosted by the EU Military Staff.

⁽¹⁾ COM(2026) 577 final.

⁽²⁾ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

⁽³⁾ Regulation (EU) 2024/2847.

⁽⁴⁾ Regulation (EU) 2024/1689.

⁽⁵⁾ COM(2026) 11 final.

⁽⁶⁾ Regulation (EU) 2021/697.

⁽⁷⁾ Regulation (EU) 2025/2643.

⁽⁸⁾ Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management.

⁽⁹⁾ JOIN(2022) 49 final.

⁽¹⁰⁾ <https://www.consilium.europa.eu/media/64526/st09618-en23.pdf>.