

(English version)

**Question for written answer E-001844/26  
to the Commission**

**José Cepeda (S&D), Elio Di Rupo (S&D), Nacho Sánchez Amor (S&D), Sven Mikser (S&D)**  
(6 May 2026)

*Subject:* European capacity for AI-driven large-scale vulnerability research and cybersecurity resilience

On 7 April 2026, the US company Anthropic announced Claude Mythos Preview, a general-purpose AI model reportedly capable of autonomously identifying and exploiting large numbers of zero-day vulnerabilities across widely used software systems.

This development highlights the growing role of AI in cybersecurity, including both defensive and offensive capabilities, in a context where the EU has identified cyber, AI and electronic warfare as priority capability domains for its security and defence.

At the same time, EU cybersecurity policy has so far focused primarily on resilience, risk management and incident response (e.g. the NIS2 Directive <sup>(1)</sup>, the Cyber Resilience Act <sup>(2)</sup>), rather than on large-scale vulnerability discovery capabilities.

Considering this evolving technological landscape:

1. What measures is the Commission taking to strengthen EU-level capabilities for large-scale, AI-assisted vulnerability research, including through the European Cybersecurity Competence Centre, the European Union Agency for Cybersecurity, Digital Europe and Horizon Europe?
2. How does the Commission assess the risks associated with a potential concentration of advanced vulnerability discovery capabilities in non-EU actors for the security and resilience of the EU?
3. Does the Commission envisage mechanisms to ensure timely access, sharing and coordinated remediation of critical vulnerabilities identified by advanced AI systems, in particular where they may affect European critical infrastructure?

Submitted: 6.5.2026

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

The Commission adopted on 7 July 2026 an Action Plan on Cybersecurity and AI with concrete actions to support Member States and organisations across the EU <sup>(1)</sup>.

A key priority is to ensure that Europe steps up its preparedness and resilience in the face of the cybersecurity risks posed by frontier AI.

Amongst other things, the action plan proposes concrete actions for the Commission, Member States and the EU Agency for Cybersecurity (ENISA) to upgrade existing vulnerability handling processes to be effective in the age of AI-assisted vulnerability discovery. The Commission also tasks ENISA to accelerate patching of vulnerabilities in the area of open source software.

A mapping of critical open source components is foreseen under the EU Open Source Strategy <sup>(2)</sup> and based on a preliminary list informed by agreed criteria, ENISA will pilot a Critical Open Source Resilience Campaign for open source components relevant to critical infrastructure.

The action plan also prioritises investments in European AI capabilities for cybersecurity with investments in research and development for homegrown advanced AI-enabled cybersecurity technologies already existing under the Horizon <sup>(3)</sup> and Digital Europe Programmes <sup>(4)</sup>. It proposes to launch an EU Grand Challenge on AI-assisted vulnerability.

<sup>1</sup> 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) (OJ L 333, 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

<sup>2</sup> Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

<sup>(1)</sup> COM(2026) 577 final.

<sup>(2)</sup> COM(2026) 503 final.

<sup>(3)</sup> [https://commission.europa.eu/funding-and-tenders/find-funding/eu-funding-programmes/horizon-europe\\_en](https://commission.europa.eu/funding-and-tenders/find-funding/eu-funding-programmes/horizon-europe_en).

<sup>(4)</sup> [https://commission.europa.eu/funding-and-tenders/find-funding/eu-funding-programmes/digital-europe-programme\\_en](https://commission.europa.eu/funding-and-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en).

In order to finance Europe's tech sovereignty ambitions, the communication on European Tech Sovereignty calls for a reflection on the means to boost a European equity capacity at scale in order to establish a portfolio of equity investments in advanced technologies and infrastructure in critical sectors, including AI <sup>(5)</sup>.

---

---

<sup>(5)</sup> COM(2026) 503 final.