

(English version)

**Question for written answer E-001575/26
to the Commission**

**Leila Chaibi (The Left), Kim Van Sparrentak (Verts/ALE), Manon Aubry (The Left), David Cormand (Verts/ALE),
Damien Carême (The Left), Fernando Barrena Arza (The Left), Elena Kountoura (The Left), Emma Rafowicz (S&D),
Arash Saeidi (The Left), Rima Hassan (The Left), Jussi Saramo (The Left)**

(16 April 2026)

Subject: Claude Mythos and the cybersecurity risks facing the EU

On 7 April 2026, Anthropic announced that it would not be releasing its upcoming artificial intelligence model, Claude Mythos Preview, to the public. According to its developers, the model's capabilities in detecting and exploiting software vulnerabilities are so advanced that Claude Mythos has already identified hundreds of critical flaws in programmes that had already undergone millions of tests.

Anthropic also announced a private initiative, Project Glasswing, enabling a select group of US companies and organisations to have their vulnerabilities remediated ahead of any public disclosure.

As the Center for AI Safety ⁽¹⁾ has noted, time is of the essence for the EU. By Anthropic's own admission, Claude Mythos holds only a six to twelve-month lead over its open-source competitors. Without an immediate and public response, the EU's digital ecosystem faces severe exposure to an anticipated surge in cyberattacks.

1. What cybersecurity strategy does the Commission intend to put in place in order to avert a potential EU 'cybergeddon'?
2. How will it support the development of a sovereign EU capability for advanced vulnerability research?
3. How does it intend to adapt the EU legislative framework to the emergence of AI models endowed with such offensive capabilities?

Submitted: 16.4.2026

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

Recent developments in frontier AI models have not come as a surprise, yet the speed and scale at which AI can detect and identify vulnerabilities present new cybersecurity risks and opportunities.

The existing EU legal framework on AI and cybersecurity provides a robust set of rules to address such risks. It is now necessary to translate this framework into operational capacity, with an urgency that reflects the threat.

On 19 May 2026, the Commission announced a dedicated Action Plan on AI and Cybersecurity ⁽¹⁾, comprising actions to step up the EU's preparedness, bringing together the best EU expertise in AI and cybersecurity, in close cooperation with like-minded partners.

It will include practical steps to help Member States, critical infrastructure operators, open-source communities and businesses manage risks, while also strengthening Europe's advanced AI cybersecurity capabilities.

It will complement and build on the existing cybersecurity framework, including the directive on a high common level of cybersecurity across the Union (NIS 2) ⁽²⁾ and the Cyber Resilience Act ⁽³⁾.

Furthermore, under the AI Act ⁽⁴⁾, providers of the most advanced AI models must notify the Commission as soon as they become aware a model meets the relevant thresholds and must assess and mitigate systemic risks, including risks of cyber misuse.

¹ Grimonpont A. and Dorn F., 'CeSIA calls for an urgent European response after the revelation of Claude Mythos' cyber capabilities', Center for AI Safety, 8 April 2026, <https://cesia.org/fr/publications/le-cesia-appelle-%C3%A0-une-r%C3%A9ponse-europ%C3%A9enne-durgence-apr%C3%A8s-la-r%C3%A9v%C3%A9lation-des-capacit%C3%A9s-cyber-de-claude-mythos/>.

⁽¹⁾ https://www.europarl.europa.eu/doceo/document/CRE-10-2026-05-19-ITM-002_EN.html.

⁽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), OJ L 333, 27.12.2022, pp. 80-152, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>.

⁽³⁾ 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>.

⁽⁴⁾ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>.

Since 2025, the AI Office has received information and held technical compliance dialogues with providers to improve their safety practices.

The Commission is also anticipating future cybersecurity needs: its proposed revision of the Cybersecurity Act ⁽⁵⁾ foresees a near-doubling of the resources of the EU Agency for Cybersecurity, and the European Competitiveness Fund, proposed in the next Multiannual Financial Framework will be critical to bolstering Europe's AI cybersecurity capabilities.

⁽⁵⁾ Proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2).