

(English version)

**Question for written answer E-001843/26
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 regulatory gap regarding offensive AI capabilities

On 7 April 2026, the US company Anthropic announced Claude Mythos Preview, a general-purpose artificial intelligence (AI) model capable of autonomously discovering and exploiting thousands of zero-day vulnerabilities across major operating systems and web browsers.

This case reveals a significant structural gap in the European regulatory framework: Article 2(3) of the AI Act ⁽¹⁾ expressly excludes from its scope AI systems used for military, defence or national security purposes, regardless of whether the operator is a public or private entity. This means that AI models with state-level offensive capabilities — including those that could potentially be deployed by private actors in defence-related contexts — may operate in a largely unregulated space at EU level.

This exclusion creates a regulatory grey area, particularly for dual-use AI systems developed by private actors, whose initial purpose is not military, but which can be integrated into offensive cyber operations or intelligence capabilities.

In the light of the above, does the Commission intend to address the gap in Article 2(3) of the AI Act with regard to AI systems with offensive cyber capabilities developed by private actors, in particular when such systems are deployed in decision-making chains affecting the security of the EU and its Member States?

Submitted: 6.5.2026

Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(7 July 2026)

Pursuant to Article 2(3) of the AI Act ⁽¹⁾, the AI Act does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification or where the output is used in the EU exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. Hence, these exemptions apply regardless of whether the deployer is a public or a private entity.

Concerning dual-use AI systems, the purpose is not exclusively for military, defence or national security purposes, so the AI Act applies for these systems.

This is clarified by Recital 24 of the AI Act: ‘AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this regulation and providers [...] should ensure compliance with this regulation’.

In the Guidelines on Prohibited AI Practices ⁽²⁾, paragraphs 24 and 25 refer to dual-use AI systems falling within the scope of the AI Act and present an example: ‘if a company offers a remote biometric identification system for various purposes, including law enforcement and national security, that company [...] must ensure its compliance with the requirements in the AI Act’.

According to the information available to the Commission, Mythos Preview has been made available to a range of business customers and cyber-defensive organisations in the course of commercial activity and is not placed on the market exclusively for military, defence or national security purposes within the meaning of Article 2(3) AI Act.

¹ 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>).

⁽¹⁾ 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>).

⁽²⁾ Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (<https://ec.europa.eu/newsroom/dae/redirection/document/112367>).