

(English version)

**Question for written answer E-003317/26
to the Commission
Fabio De Masi (NI)
(24 August 2026)**

Subject: Legal accountability and preventive measures for cybersecurity breaches caused by autonomous AI systems

Recent incidents involving highly capable AI systems have demonstrated that autonomous systems may identify and exploit vulnerabilities, access external systems and cause cybersecurity breaches in ways that were not explicitly designed or anticipated by their developers ⁽¹⁾ ⁽²⁾ ⁽³⁾.

In such circumstances, it appears that European regulation has so far been inadequate in identifying legal responsibilities and preventing such incidents. In this respect, Article 2(8) of Regulation (EU) 2024/1689 ⁽⁴⁾ excludes from the scope of the AI Act research, testing and development activities concerning AI systems or AI models prior to their being placed on the market or put into service.

In the light of the above, we pose the following questions to the Commission.

1. Do any of the activities involved in the OpenAI and Anthropic incidents, as described above, fall outside the scope of the AI Act under Article 2(8)?
2. What supervisory action has the Commission taken, or what action does it intend to take, in response to these incidents under its existing powers?
3. Does the Commission consider that the existing EU legal framework provides sufficiently clear rules establishing responsibility and liability where an autonomous AI system, during research, testing or development, independently exploits a cybersecurity vulnerability and causes damage to a third party?

Submitted: 24.8.2026

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

The AI Act covers autonomous AI systems and AI agents in accordance with the definitions of AI system and general-purpose AI model ⁽¹⁾.

Providers of general-purpose AI models with systemic risk should ensure that systemic risks, including cyber risks and loss of control, are continuously assessed and mitigated across the entire model lifecycle, starting from the large pre-training run ⁽²⁾.

The AI Office has requested and received serious incident reports in relation to recent loss of control incidents and has asked further questions to the providers.

Based on its assessment of providers' replies, the AI Office will determine whether further enforcement action is necessary. In accordance with the AI Act, the AI Office may issue requests for information by decision, if providers refuse to answer or provide incomplete answers; request access to models to conduct evaluations; require providers to implement appropriate mitigating measures; and where necessary, restrict the making available of a model on the market. The AI Office may also issue fines if providers provide incorrect or misleading information.

The Commission is ready to take the necessary steps to make sure companies comply with their obligations. The enforcement powers of the Commission with regard to the AI Act ⁽³⁾ entered into application on 2 August 2026.

¹ <https://www.bbc.com/news/articles/cz7dl7w8y7po>.

² <https://edition.cnn.com/2026/08/04/tech/ai-anthropic-openai-security-breach-intl-hnk>.

³ <https://www.bbc.com/news/articles/c2el319vzr3o>.

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>).

⁽¹⁾ <https://ai-act-service-desk.ec.europa.eu/en/faq>.

⁽²⁾ Article 55 AI Act; Section 2.2 of the Commission Guidelines on the scope of the obligations for providers of general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act), <https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act>.

⁽³⁾ <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

Building on Europe's unique legal framework for AI, which is at once risk-based and containing comprehensive AI and cybersecurity rules, on 7 July 2026, the Commission adopted an Action Plan on Cybersecurity and AI with the aim to ensure, amongst other things, that frontier AI models are safe, accessible and deployable for cybersecurity in Europe, and to prepare the EU's cyber ecosystem for the challenges and opportunities of increasingly cybercapable AI ⁽⁴⁾.

⁽⁴⁾ COM(2026)577 final.