

EN

E-002609/2026

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(5.10.2026)

As advances in frontier AI models offer opportunities as well as novel and heightened risks for cybersecurity, the Commission adopted on 7 July 2026 an Action Plan on Cybersecurity and AI¹. A key priority of the Commission is to ensure that frontier AI models are safe, accessible and deployable for cybersecurity in Europe.

The Action Plan proposes a Blueprint as a framework for structured access to advanced AI capabilities for cybersecurity purposes which will include criteria that should be considered for granting access to European players. As part of the Blueprint, the Commission intends to propose processes and restrictions on the handling of information such as prompts, uploaded files and outputs, thus also ensuring the privacy and safety of potentially critical European information.

The ability to develop and deploy AI-powered cybersecurity solutions is becoming a strategic enabler of cyber resilience and sovereignty. As part of the Tech Sovereignty Package of 3 June 2026, the Commission proposed the Cloud and AI Development Act² which would expand EU data centre capacity and cloud and AI autonomy, supporting the wider deployment of AI – including cyber-related tools and applications. The Action Plan aims to scale European AI capabilities for cybersecurity. This includes boosting the European ecosystem around AI-powered cybersecurity solutions, e.g. through the grand challenge on AI-assisted vulnerability remediation, building European frontier capabilities and boosting cybersecurity skills for the age of AI. In the meantime, European players should already start using available AI capabilities, including through open-source models, to detect vulnerabilities and to improve the detection and prevention of cyberattacks.

¹ COM(2026) 577 final.

² COM(2026) 502 final.