European Commission

European Commission - Speech

[Check Against Delivery]

Remarks by Executive Vice-President Virkkunen on the Action plan on Cybersecurity and Artificial Intelligence

Strasbourg, 7 July 2026

Advanced AI models create many possibilities. They can help us to prepare and protect but they can also be used against us.

Advanced AI can create cyber exploits in just minutes or hours, for a fraction of the cost of human experts. While a major vulnerability can cost over 1 million EUR on the grey market, AI only needs data center compute power. Once weaponised, these flaws can endanger our infrastructure and society, which is built upon digital systems.

The Commission's response has been immediate. We engaged with the entire AI and cybersecurity ecosystem: with Member States, with AI providers, with industry, and with our international partners.

We are not starting from scratch. The EU already has robust legal and policy foundations to address these challenges. We are now turning them into action, capability, and resilience, along three priorities.

First, AI models with high cyber capabilities must be safe. And Europeans must have access to use them.

Through the AI Act, the EU has the world's strongest framework to protect us from the potential risks of advanced AI. The Commission's AI Office is already working with AI companies to implement these rules.

Under the AI Act, advanced AI models must be evaluated, and mitigation measures carefully assessed, before the models are placed on the EU market.

In less than a month, the AI Office will have enforcement powers. Testing models before they are released is key to reducing risk. To build expertise, the EU will launch a call to boost its AI evaluation capacity—especially in cybersecurity—aiming to be operational by 2027.

The EU Agency for Cybersecurity, ENISA, will play an important role in operationalising this Action Plan, as well as some Member States.

Together with ENISA, we will develop a European Blueprint for structured access to advanced AI models, with focus on cybersecurity.

The Blueprint will support both AI providers and European organisations, including companies, on how to identify those who get access and on which terms. It will also serve as a basis for cooperation and alignment with international partners.

But access is not enough. We must also strengthen our know-how on how to deploy these technologies for our cybersecurity, by testing their cyber capabilities.

This is why the Commission will set up a secure platform to test AI for cybersecurity already by the end of 2026.

The platform will allow us to assess how models can be used safely for cybersecurity operations in critical sectors such as finance, energy, health, transport or public administration.

Second, we must also be able to protect ourselves against malicious attacks stemming from the misuse of such models.

Our immediate priority is clear: identify and fix the most critical vulnerabilities faster. The first step is the full and effective implementation of our cybersecurity legislation: the NIS2 Directive, DORA, and

the Cyber Resilience Act.

This applies to all member states – I want to take the opportunity to highlight the urgency of implementing especially the NIS2 directive.

But we also need targeted action where exposure is the highest for our critical infrastructure. We will therefore launch a Critical Open Source Resilience Campaign, to support maintainers in fixing the most critical vulnerabilities in key open-source projects.

AI is not only a risk: it is also a strategic enabler of cyber resilience. Existing AI tools can already help with vulnerability management, threat detection, and incident response. We must support their safe and secure uptake across critical sectors, SMEs and public authorities. And we must do so fast.

Third, we must build Europe's own AI-powered cyber capabilities.

We cannot rely only on non-European solutions for capabilities that are critical for our security.

Building up our own AI frontier models is costly, but in today's world, the cost of not building them will be even higher.

Frontier AI requires very large-scale investment, far beyond what public funding alone can provide. We need to mobilise private capital, and especially equity. The new European tech equity capacity announced in the Tech Sovereignty Package can be a game changer here.

Europe has what it takes to compete. We have the talent. We have a solid cybersecurity and AI ecosystem. We have AI Factories and, in the future, AI Gigafactories that can be part of a sovereign European infrastructure for AI and cybersecurity.

SPEECH/26/1546

Press contacts:

Thomas REGNIER (+32 2 29 91099)
Patricia POROPAT (+32 2 29 80485)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Related media

EC press conference by European Commission Executive Vice-President Henna VIRKKUNEN on the Action plan on Cybersecurity and Artificial Intelligence