European Parliament

Executive Vice-President Henna Virkkunen
Executive Vice-President for Tech Sovereignty, Security and Democracy
European Commission
Rue de la Loi 200, B-1049 Brussels

Brussels, 4 May 2026

Subject: Urgent Call for a European AI-Cybersecurity Mitigation Plan

Dear Executive Vice-President Virkkunen,

We write to you with urgency regarding an emerging threat to European cybersecurity. Advanced AI systems, such as Anthropic's Mythos, are fundamentally altering the cyberattack landscape by automating the discovery and exploitation of software vulnerabilities at unprecedented speed and scale. Already, financial officials have warned that this model could threaten the world banking system. A race against time has begun, and Europe is not yet prepared.

Reports of unauthorised access to Mythos underscore that this threat is no longer hypothetical. What we are witnessing is not specific to Mythos: it marks a turning point. Many other capable AI models are emerging and open-source equivalents such as Kimi K2.6, when combined with agentic systems, are poised to lower the barrier to sophisticated attacks even further. Public services and critical infrastructure across Europe face risks of a scale and speed we have not previously encountered.

Anthropic's Project Glasswing, the industry-led initiative to proactively patch vulnerabilities, demonstrates the willingness of AI and cybersecurity companies to take responsibility. Regrettably, it does not include any European institution or company, nor the organizations that steward the open-source internet infrastructure.

The NIS2 already requires critical entities to adopt a zero-trust architecture, a breach mindset, and an active defensive stance. But our existing cybersecurity frameworks are ill-equipped for systems with this level of capability. We therefore call on the Commission to carry out a European mitigation plan:

- Engage Anthropic and frontier AI developers to ensure European participation in Project Glasswing and equivalent initiatives in order to secure early access to AI models (also by ENISA);
- Accelerate adoption of Zero Trust architectures, assume-breach principles, and AI-assisted defensive tools, with concrete guidance for both public institutions and private enterprises;
- Reform vulnerability disclosure and patching frameworks to reflect compressed AI-driven timescales, enabling rapid and pre-emptive patching, including beyond organisations' own networks where appropriate;
- Promote immediate reduction of attack surfaces, further network segmentation, and prioritising the protection of crown jewels.

We do not call for restrictions on the use of AI-powered cybersecurity measures in Europe as they are equally indispensable to our defence. We kindly ask you to respond to this letter as a matter of priority, setting out the concrete steps the Commission intends to take. Businesses and governments across the Union need guidance to act now, before the window to prepare closes.

Yours sincerely,

Bart Groothuis, Renew Europe

Markéta Gregorová, Greens/EFA

bart.groothuis@europarl.europa.eu

Jens Geier, S&D

Hildegard Bentele, EPP

Kathleen van Brempt, S&D

Ondřej Krutílek, ECR

Matthias Ecke, S&D

Dirk Gotink, EPP

Lukas Sieper, Renew Europe

Irena Joveva, Renew Europe

Kim van Sparrentak, Greens/EFA

Ivars Iljabs, Renew Europe

Morten Løkkegaard, Renew Europe

Joao Cotrim de Figueiredo, Renew Europe

Petras Austrevicius, Renew Europe

Karin Karlsbro, Renew Europe

Bert-Jan Ruissen, ECR

Veronika Cifrová Ostrihoňová, Renew Europe

Malik Azmani, Renew Europe

Lucia Yar, Renew Europe

Merja Kyllönen, the Left

Engin Eroglu, Renew Europe

Sergey Lagodinsky, Greens/EFA

Jan-Christoph Oetjen, Renew Europe

Nathalie Loiseau, Renew Europe

Jeanette Baljeu, Renew Europe

Ana Vasconcelos, Renew Europe

Leïla Chaibi, the Left

Michael McNamara, Renew Europe

Anouk van Brug, Renew Europe