26 May 2026

Open Letter on the Emergence of "Mythos"-Class AI Cyber Capabilities

Dear Colleagues, Partners, and Stakeholders,

Europe's airports operate in an increasingly complex geopolitical environment marked by persistent cyber threats and hybrid warfare activities.

In this context, recent developments around "Mythos"-class artificial intelligence capabilities (AI systems able to autonomously identify, chain and exploit vulnerabilities at unprecedented speed and scale) represent a significant evolution in the cyber risk landscape.

As airport environments are highly complex ecosystems involving operators, airlines, ground handlers, industrial systems, cloud services, software vendors, and a large number of technology and service providers, this challenge is particularly relevant. A weakness introduced anywhere in this supply chain can have operational consequences far beyond a single organisation.

The emergence of Mythos-class threats makes clear that cybersecurity resilience must now be collective across the entire aviation ecosystem. Therefore, ACI EUROPE expects all technology partners, managed service providers, software suppliers, and relevant actors supporting and involved in airport operations to actively anticipate this new generation of AI-enabled threats and implement appropriate mitigation measures without delay.

This includes in particular:

1. Reduced attack surface exposure;
2. Reinforced identity, segmentation, and zero-trust principles;
3. Risk based Vulnerability Management Process – Risk = Severity (CVSS) + Exploit Prediction (e.g. EPSS) + Exposure (e.g. to the internet) + Business Impact (e.g. Confidentiality, Integrity, Availability);
4. Strong software supply chain security able to meet as early as possible the EU Cyber Resilience Act requirements and objectives (entry into force September 2027). This in turn requires:
    - Fast, effective and fully transparent
        - vulnerability disclosure program
        - remediation mechanism.
    - Remediation to be prioritized based on a Risk-based Vulnerability Management approach
    - Establishing and maintaining a Software Bill of Materials (SBOM)
    - Automated defensive security testing
5. Where possible, effective detection and remediation using "Mythos"-class AI tools:
    - for all future products and services
    - in retrofit program to discover hidden existing vulnerabilities
6. Robust resilience and recovery capabilities.

Airports Council International – European Region AISBL
37 Boulevard du Régent, 1000 Brussels, Belgium - tel: +32 (0)2 552 0980 - fax: +32 (0)2 502 5637
e-mail: olivier.jankovec@aci-europe.org - **www.aci-europe.org** - TVA: BE 431.887.748

The aviation sector has always demonstrated resilience in the face of evolving risks. With the right level of cooperation, transparency, and shared responsibility across the entire ecosystem, airports remain confident in their ability to adapt to this new cybersecurity environment.

Olivier Jankovec
Director General
ACI EUROPE