1 July 2025 |

ASD Input on the Cloud and AI Development Act

POSITION PAPER

1. Introduction

The European Commission published the AI Continent Action Plan ('the Plan') on 9 April,[1] setting out an ambitious vision to position the European Union as a global leader in artificial intelligence. The Plan encompasses five key areas: computing infrastructure, data access, AI adoption in key sectors, talent base and regulatory simplification. The Aerospace, Security and Defence Industries Association of Europe (ASD) welcomes the European Commission's initiative.

The Communication on the AI Continent Action Plan includes a public consultation on the upcoming Cloud and AI Development Act ('the Act'), which falls under the "Computing infrastructure" pillar. This document sets out our key recommendations to ensure that the Act adequately addresses the strategic, operational and security-specific requirements of the defence and security sectors. Given that civil aviation is already governed by established regulatory and standardisation frameworks, such as those of the European Union Aviation Safety Agency (EASA) and standard-developing organisations like EUROCAE, it is not addressed within the scope of this paper.

Digital infrastructure is not only a driver of innovation in these domains, but a matter of national and European sovereignty. Cloud computing, in particular, has emerged as a strategic asset for the defence and security sectors. It underpins secure data sharing, AI-driven systems, cross-border collaboration, and mission-critical operations. However, the European Union (EU) remains heavily reliant on non-European cloud providers, with U.S.-based hyperscalers dominating the market. This structural dependency poses serious risks to the EU's digital autonomy, especially as geopolitical tensions and cyber threats increase.

For Europe to maintain its technological sovereignty, especially in highly sensitive sectors, a secure, sovereign, and interoperable cloud ecosystem is essential. This paper outlines the current challenges,

[1] European Commission (2025), *Commission sets course for Europe's AI leadership with an ambitious AI Continent Action Plan*, <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1013>.

highlights strategic capability gaps, and offers concrete policy and technical recommendations to ensure the EU's digital infrastructure is equipped to support next generation defence and security applications.

2. Cloud as a strategic asset for aerospace and defence

The AI Continent Action Plan rightly highlights a critical vulnerability: the European Union lags behind the United States and China in data centre capacity. At present, the EU remains heavily reliant on cloud infrastructure that is either physically located outside its territory and/or controlled by non-European entities. The EU cloud services market is currently disproportionately dominated by non-EU providers, with the three major US-based cloud 'hyperscalers' accounting for 65% of the market share.[2]

This structural dependency is a serious concern for European industry, public institutions, and the EU's long-term digital sovereignty. In particular, it entails the risk of service disruption due to extraterritorial legislation or influence from non-EU countries, notably through undue access to data or adverse impacts on the quality and/or availability of the provided service.

Mario Draghi emphasizes in his report the urgent need for the EU to maintain its technological sovereignty, including in cloud services. For the security and defence sectors, which increasingly rely on data flows, AI-driven capabilities, and secure information-sharing, this challenge is particularly acute. Cloud services are essential for innovation, operational readiness and secure cross-border collaboration. We therefore strongly support the Plan's emphasis on developing sovereign, highly secure, EU-based cloud capabilities for highly critical use cases.

3. Cloud and technological sovereignty: key concerns

The security and defence industries have a vested interest in advancing the EU's technological sovereignty. This is not only a matter of industrial competitiveness, but a critical requirement for secure, resilient and future-ready defence capabilities.

Several key concerns must be addressed in the context of the Cloud and AI Development Act:

- **High security and resilience requirements:** defence systems require cloud and edge infrastructures that meet stringent demands for security, availability, and confidentiality needs.

[2] European Commission (2024), *The future of European competitiveness: Report by Mario Draghi*, p. 77, <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en>.

- **Interoperability across actors and borders:** modern defence programmes involve a diverse and evolving network of stakeholders such as Ministries of Defence (MoDs), industrial partners, SMEs, and technology providers across Member States. Interoperability of data, tools and platforms is essential, yet current cloud and edge solutions fall short of enabling this level of collaboration at scale.
- **Fragmentation of rules and standards:** the absence of a unified EU accreditation framework and consistent cloud standards across Member States hinders collaboration and slows deployment. A joint European approach is urgently needed to streamline compliance and certification, particularly for defence-related cloud applications.
- **Gaps in specific military programmes:** existing cloud and edge technologies do not adequately support the long-term requirements of military systems. This shortfall undermines the long-term competitiveness of the European defence technological and industrial base (EDTIB), despite the European Union being a major provider of information technology.
- **Disjointed digital regulatory environment:** while initiatives such as the General Data Protection Regulation (GDPR), the Data Act, the AI Act or Gaia-X are important, they do not fully address the specific requirements of European defence programmes.
- **Barriers to digital transformation and innovation:** the absence of secure, shared IT infrastructure across the EU hampers the adoption of modern systems engineering methods (e.g., Agile, DevSecOps), which are essential for developing future-ready military capabilities.

4. Strategic capabilities for a sovereign European cloud ecosystem

To address the structural and operational limitations outlined above, the European Union should take decisive steps to further consolidate its technological sovereignty in cloud computing, a foundational layer of digital infrastructure across all sectors. A secure, resilient, and interoperable European cloud ecosystem is essential to enable digital autonomy, ensure data control, and support mission-critical operations. In the defence, and security sectors in particular, several technical and policy priorities stand out:

- **Trusted Identity and Access Management (IAM):** a federated and secure IAM framework is essential for operating across multi-cloud and hybrid environments. It must ensure robust traceability, strong authentication, and role-based access control across distributed infrastructures.
- **End-to-end protection:** fully trusted encryption, including advanced technologies such as homomorphic encryption, is critical to ensuring data privacy, especially when handling sensitive or classified information across jurisdictions and distributed systems.

- **Transparent and modular cost models:** defence programmes require cloud billing systems that allow granular cost attribution based on usage, service type, and mission-specific requirements. Such models support both budgeting flexibility and operational accountability.
- **Multi-cloud service catalogues with guaranteed service levels:** a common, EU-managed catalogue of sovereign cloud services, listing European providers that meet the criteria of the certification scheme mentioned below, and offering clearly defined service level agreements (SLAs) would streamline procurement, build trust, and facilitate cross-border integration of cloud-based systems in defence and aerospace programmes.
- **Unified management experience:** simplifying user interfaces and operational workflows across cloud providers e.g., through orchestration layers or common management portals would support more agile development and deployment across the EU ecosystem.

5. Barriers to cloud adoption

One of the most significant challenges to cloud adoption in the European defence and security sectors is the lack of harmonised security standards, particularly regarding the handling of classified and sensitive data.

Several key obstacles must be addressed:

- **Absence of European-wide convergence on data classification and protection:** while "EU restricted" is defined under European Classified Information (EUCI), multiple national-level classifications or security markings remain in use across Member States e.g., "Diffusion Restreinte" (France), "Difusión Limitada" (Spain), "Riservato" (Italy), "VS-NfD" (Germany), OCCAR Restricted, and NATO Restricted. These classifications lack mutual recognition mechanisms and harmonized standards for cloud compliance.
- **Lack of an EU-wide certification scheme for sovereign cloud services:** the absence of such a certification scheme creates legal uncertainty and limits the ability of customers to assess EU sovereignty guarantees. Addressing this shortfall is essential to accelerate the adoption of European cloud infrastructure and to foster a thriving "cloud BY Europe" ecosystem. The EUCS High+ criteria can serve as strong inspiration in this regard. The assessment could be based on:
    - The location of the provider's head office and central administration within the EU.
    - The place where key operational and management decisions are made.
    - The service provider is not controlled, even jointly, by non-EU stakeholders.

  This approach would help ensure that security and compliance functions align with the underlying sovereignty objectives. Additionally, consideration should be given to whether non-

EU actors could, through other means e.g., specific restrictions, impede the provision or quality of the service. In other words, the criteria, subject to refinement, should guarantee immunity from non-EU extraterritorial reach, both regarding undue access to data and potential disruption of service.

- **Absence of sovereign criteria for public procurement:** this shortfall not only exposes public administrations to significant risks but also hampers the development of "cloud BY Europe" services, which are increasingly essential for highly critical industrial use cases. Therefore, sovereignty criteria for public procurement should be established at the EU level, proportionate to the sensitivity of the data involved. Importantly, these criteria should encompass all aspects of sovereignty outlined above to prevent non-EU extraterritorial disruption or data access. Accordingly, these criteria should be similar to the EUCS High+ requirements described earlier. In addition, the absence of certification criteria, similar to the EUCS High+, for a sovereign cloud for all other use cases in industry and services, particularly regarding collaborative engineering for defence programs, is equally a barrier to European collaborative initiatives and enterprises.
- **No unified EU body to certify cloud technologies for restricted defence data:** each Member State currently operates its own national cybersecurity authority (e.g., ANSSI in France, CCN in Spain, BSI in Germany, UCSE in Italy). However, there is no pan-European mechanism to jointly assess or certify IT products, particularly cloud services, for use with EU or nationally restricted data.
- **Cloud incompatibility with high-level national classifications:** more sensitive classifications, such as "Secret Défense" or "Très Secret Défense" in France, are explicitly incompatible with current commercial cloud offerings or connected AI systems. At present, no technological solution exists that fully meets national-level security requirements for handling such data in the cloud.
- **Proliferation of national caveats (e.g., "Eyes Only"):** country-specific access restrictions, such as "German Eyes Only" or "Italian Eyes Only", further fragment the landscape. Currently, there are no agreed-upon mechanisms or trusted infrastructure to enforce and respect these caveats within multi-national, cloud-based environments.

6. Conclusion

The Cloud and AI Development Act represents a strategic opportunity for the European Union to address critical gaps in digital infrastructure and strengthen its technological sovereignty, particularly in high-stakes sectors such as defence and security. ASD strongly supports the ambition of the AI Continent Action Plan and calls for the Act to incorporate the sector-specific requirements outlined in this paper.

To ensure Europe leads in trusted AI and cloud solutions, we urge the European Commission to prioritise harmonised security standards, applicable to both sensitive data and public procurement, that protect against non-EU extraterritorial access or disruption. This should be complemented by interoperable cloud frameworks, sustained support for defence programmes, and the development of sovereign infrastructure. A coherent, European-driven cloud ecosystem built on secure, certified, and inclusive foundations is essential for the resilience of our industries and the Union's strategic autonomy.

CASE STUDIES

Our industry is taking steps to address the lack of a trusted, interoperable, and secure European cloud environment tailored to defence and aerospace needs. Here below are several case studies:

- **AEROSEC**

Airbus, Dassault Aviation, Dassault Systèmes, Indra, Leonardo, and Outscale are cooperating on the AEROSEC project, a European industry initiative aimed at developing a sovereign, secure, and federated cloud platform for defence applications. AEROSEC focuses on enabling a common framework for secure data sharing, federated identity and access management, and multi-cloud capabilities across national and industrial boundaries. The project is expected to deliver demonstrators in areas such as identity accreditation for multi-cloud security, secure multi-cloud communication services, and digital model-based systems engineering.

- **3DEXPERIENCE**

In June 2023, Dassault Aviation and Dassault Systèmes announced a partnership to develop a secure, sovereign cloud environment tailored for next-generation defense programs, notably the Future Combat Air System (FCAS). This initiative leverages Dassault Systèmes' 3DEXPERIENCE platform, operated on OUTSCALE, a Dassault Systèmes brand, which has achieved the SecNumCloud 3.2 qualification from the French National Cybersecurity Agency (ANSSI), representing the highest level of security recognition in France.

- **MILSCA**

In February 2024, Leonardo initiated the MILSCA project, aiming to define a space-based cloud architecture capable of providing high-performance computing and storage directly in space for

defence applications. This project, assigned by the Italian Ministry of Defence, seeks to enhance the speed and flexibility of data processing and sharing for military operations.

- **FCAS**

Airbus, alongside Dassault Aviation and Indra, serves as a national industrial coordinator for the Future Combat Air System (FCAS) program. Airbus is leading the development of the Combat Cloud pillar, which aims to provide a decentralized, cyber-resilient, collaborative information network across multiple domains (air, land, sea, space, and cyber) using cloud-based technologies.

- **EDINAF**

Under the 2021 EDF project EDINAF, a consortium of major European shipbuilders incl. Damen, Fincantieri, Naval Group, Navantia, Saab, and TKMS, began developing a reference digital architecture for warships. This architecture is designed to provide a coherent set of resources, services, and data solutions that support core naval operations. The follow-up to this project, set to begin in 2027, will define the reference architecture for the Naval Combat Cloud. Building on a cyber-secure, cloud-oriented ship digital architecture, this next phase will focus on tactical-level capabilities and take a holistic approach to meeting military naval requirements.

***

[*Signed by*], Jan Pie, Secretary General of ASD

Brussels, 03 July 2025