egis

MILITARY AND U-SPACE: GUIDELINES

SC4 FINAL REPORT

17 September 2024

EUROPEAN DEFENCE AGENCY

Document information

GENERAL INFORMATION

Author(s)	Stephane BERNARD (Egis) Jab CERNAN (Egis) Herve DREVILLON (Egis) Sabina ZAHARESCU (Egis)
Version	V1.0
Reference	TLSE/C4064/N240019

HISTORY OF CHANGES

Version	Date	Drafted by	Checked by	Changes
V0.1	14-Feb-2024	Stephane BERNARD Jab CERNAN Herve DREVILLON Sabina ZAHARESCU	Herve DREVILLON	Initial version
V0.2	08-Mar-2024	Stephane BERNARD Jab CERNAN Herve DREVILLON Sabina ZAHARESCU	Herve DREVILLON	First complete draft of sections 1-4
V0.3	14-Aug-2024	Stephane BERNARD Jab CERNAN Pascal DE KETELAERE Herve DREVILLON Théo FRANCOIS Sabina ZAHARESCU	Herve DREVILLON	Complete draft sent to EDA for external review
V1.0	17-Sep-2024	Herve DREVILLON	Herve DREVILLON	Version delivered to EDA (no change compared to v0.3)

RECIPIENTS

Name	Entity
Nathalie HASEVOETS	European Defence Agency

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 - EXECUTIVE SUMMARY

1.1 - Overview of the “Military and U-space: guidelines” study

The “Military and U-space: guidelines” study consists of 4 Specific Contracts (SC1, SC2, SC3, SC4) that all contribute to informing the military on their future relation with, and potential involvement within, U-space in order to preserve national and security defence requirements and to raise the awareness of the organisations implementing U-space about military needs and constraints. Each SC has its respective deliverables and the whole study is structured as depicted in Figure 1.

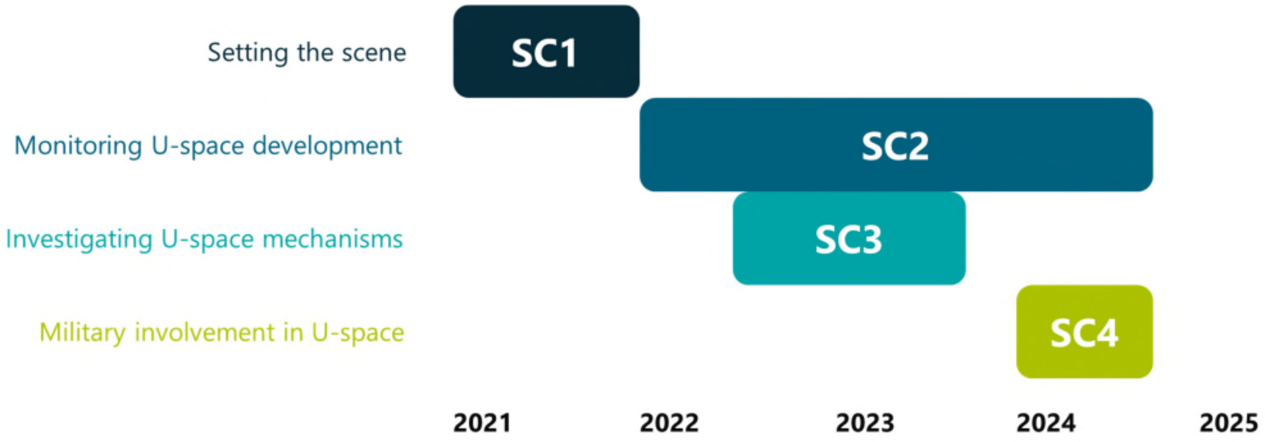


FIGURE 1: STRUCTURE OF THE “MILITARY AND U-SPACE: GUIDELINES” STUDY

1.1.1 - SC1 – setting the scene

SC1 represented the first phase of the study and aimed at developing awareness and consensus on the role of the military with regard to U-space development, based on an impact assessment covering operational, technical and financial aspects. SC1 led to the development of three main deliverables:

- D1: U-space evaluation, including the military U-space Use Cases;
- D2: financial costs calculation for the military from the U-space implementation; and
- D3: military guidelines and recommendations for further U-space involvement and engagement with the civilian stakeholders.

The first deliverable, D1, assessed both the benefits and potential negative impacts of planned, under implementation, or implemented U-space services on military missions. It analysed the U-space regulatory framework and other research activities to summarise the current direction of U-space, noting that current initiatives are primarily civilian-centric. Part of the findings is that effective civil-military coordination and cooperation will be crucial to maintaining safe and efficient operations in shared airspace.

The impact assessment determined that civilian use of U-space services will not significantly harm military missions, provided that military Airspace Management Cells (AMC and Aeronautical Information Services (AIS) processes are expanded to include U-space airspaces. The development of drone traffic, even outside U-space, poses recognised safety and security issues. However, U-space services like geo-awareness and UAS flight authorisation could enhance the safety of military missions conducted at very low altitudes compared to non-U-space environments. Military Use Cases were analysed to detail how U-space services will affect typical military activities, identifying gaps in information regarding military interaction with U-space and suggesting mitigation strategies.

Secondly, the D2 analysis focused on creating a cost benefit analysis (CBA) to understand the costs implied for the military in adapting to U-space services. It distinguished between investments in Air Traffic Management (ATM) systems, data exchanges, aircraft equipment, process reviews, staff-related costs, and studies. Although precise implementation requirements are still undefined and Member States' investment needs require further study, the CBA framework enabled the calculation of monetary values. Whatever the approach adopted by the military to collaborate with U-space, the CBA outcomes were showed to be negative, as this meant investing on the military side with very limited financial returns. However, D2 also provided an overview of European funding mechanisms for developing technological and defence capabilities, civil-military collaboration, and implementing ATM capabilities, thus identifying ways to reduce the weight of investments on the military.

Finally, based on the findings from D1 and D2, an initial set of recommendations and a proposal for a Common Military Position (CMP) on U-space development were formulated. These recommendations considered the possible outcome should the military ignore ongoing U-space developments and suggested a number of principles and actions at the policy, strategy, operational and technical levels allowing the military to limit the impact of U-space on their operations and to rather benefit from this new environment.

1.1.2 - SC2 – monitoring U-space development

Considering that the development of U-space is an on-going process, a primary objective of SC2 was to monitor U-space activities and to inform EDA and its Member States about the progress of U-space definition and implementation.

In addition, at the start of SC1 in January 2021, the U-space regulatory package had not yet been adopted and EDA anticipated that the development and implementation of U-space would be a long-term process requiring to revisit the initial work performed in SC1. Under SC2, the deliverables developed during SC1 were therefore regularly updated to reflect the state of U-space implementation across Member States, considering such aspects as policy, regulation and initial operations. This allowed to confirm, or adjust, the assumptions taken during the development of the SC1 deliverables, to review on a regular basis the proposal for a CMP developed in SC1 and to identify any need for change resulting from the progress in the definition of the U-space framework (e.g. Drone Strategy 2.0 adopted in November 2022, Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 issued in December 2022).

1.1.3 - SC3 – investigating U-space mechanisms

The goal of SC3 was to investigate in detail the applicability to military operations of two U-space mechanisms required by the U-space regulatory package: the electronic conspicuity of manned aircraft and the dynamic reconfiguration of U-space airspace. A second objective of SC3 was to develop proposals for the military to adapt to, and potentially benefit from, these mechanisms, in particular in uncontrolled airspace.

The primary objective of the e-conspicuity task was to evaluate existing electronic conspicuity systems deployed on military aircraft in light of U-space requirements. Although military aircraft are exempt from U-space regulations, aligning current equipage with U-space standards could potentially mitigate future operational and financial burdens. The analysis highlighted that while ADS-B out is available on a portion of military aircraft, full compliance with the Automatic Dependent Surveillance-Light (ADS-L) concept put forward by EASA to ensure e-conspicuity of manned aviation in any airspace, and in particular in U-space airspace, would necessitate substantial investment. Other ADS-L-compliant technologies, SRD 860 and mobile telephony, offer cost-effective options but may not universally suit military operational needs. Consequently, the report recommends leveraging strategic and tactical airspace management strategies to enhance military operational safety within U-space airspaces where no Air Traffic Services (ATS) are provided.

The second part of SC3 focused on Dynamic Airspace Reconfiguration (DAR), a process facilitating coordination between Air Traffic Control and U-space Service Providers (USSPs) to segregate manned aircraft from drone traffic within U-space. While acknowledging Member States' responsibility in defining dynamic restrictions, the report underscores challenges in applying similar measures to military flights. Indeed, military operations can occur on short notice and without the ability to inform other airspace users in a timely manner, posing complexities in coordinating effectively with USSPs.

To address these challenges, the report proposes an initial approach emphasising flexible, dynamic, and cost-effective airspace management in Very Low Level (VLL) airspace. This approach advocates for strategic/pre-tactical airspace management through information sharing and proposes providing military operational units with systems allowing interacting with CISPs/USSPs for tactical management. By leveraging principles from

Flexible Use of Airspace and DAR, this approach aims to minimise disruptions to current military operations while enhancing operational safety and efficiency within U-space.

1.1.4 - SC4 – military involvement in U-Space

The goal of SC4 was to thoroughly assess how the military could actively participate in overseeing daily manned aircraft and drone operations within U-space. Given U-space's reliance on advanced technology, automation and digitalisation, this involvement would entail sharing operational data between military and U-space systems. SC4 aimed to outline various options for military involvement and evaluated them based on factors such as personnel requirements, technological needs, financial considerations, legal aspects, and operational effectiveness. The outcome of SC4 is detailed in the following section.

1.2 - Key SC4 takeaways

- The Drone Strategy 2.0 [1] put forward by the European Commission at the end of 2022 recognises the pioneering role of the military in developing drone technologies and operations and identifies a number of flagship actions aiming, inter alia, to facilitate the integration between manned and unmanned traffic in U-space airspace and to exploit civil-defence industry synergies. Therefore, the scope and methodology of SC4 aligned perfectly with the core objectives of the European Commission's strategy, as it aims to foster synergies between the military and civilian while exploring dual-use solutions.
- SC4 delved into the landscape of potential military involvement in U-space, presenting five distinct operational scenarios that span a spectrum of responsibilities. These scenarios range from the management of UAS geo-zones to envisioning the military as both consumers and providers of critical information within U-space operations. Furthermore, SC4 underscored the possibility of the military engaging in a broader pan-European U-space organisation, emphasising the need for strategic foresight in defining its roles and responsibilities within this evolving domain.
- SC4 analysed the implications of military involvement across the identified scenarios. This assessment was conducted through a comprehensive framework that encompasses governance, regulatory considerations, operational requirements, technological capabilities, financial considerations, and the requisite workforce adjustments. By scrutinising each aspect through this multifaceted lens, SC4 provided a nuanced understanding of the challenges and opportunities that accompany military integration into U-space operations.
- Drawing inspiration from the strategies employed by civilian Air Navigation Service Providers (ANSPs), SC4 formulated business models tailored to the needs of military engagement in U-space. By correlating potential military actions, implications, and activities with established civilian frameworks, these adapted business models offer invaluable insights into the strategic alignment necessary for effective military participation in U-space. This approach ensures that military strategies are not only feasible but also aligned with broader industry practices, thereby enhancing interoperability and efficiency.
- Recognising the critical importance of interoperability between military ATM systems and U-space infrastructure if the military were to become actors in U-space, SC4 emphasised the need for a robust technical architecture. By outlining the specific interoperability requirements and technical specifications, SC4 laid the groundwork for seamless integration between military and civilian U-space systems. Moreover, by providing high-level technical architecture descriptions, SC4 provided initial recommendations for the development of interoperable solutions that would enhance the overall effectiveness of U-space operations.
- In addition to assessing the operational and technical aspects, SC4 conducted a comprehensive financial analysis to evaluate the costs and benefits associated with military integration into U-space operations. This analysis focused on identifying the investments required to support military engagement across the identified scenarios, including infrastructure upgrades, technology investments, and workforce training. By quantifying the potential costs and benefits, SC4 enabled informed decision-making and resource allocation, ensuring that military involvement in U-space is both economically viable and strategically advantageous.

2 - INTRODUCTION

The European Defence Agency (EDA) has initiated the "Military and U-space: guidelines" study in January 2021 to assess military impacts and cost benefits of large-scale drone operations. Understanding normal/nominal operations in a U-space "eco-system" is a prerequisite for the military to collaborate in U-space concept development.

The present report presents the conclusions and recommendations of the 4th Specific Contract (SC4) carried out under the study, which consists in a detailed assessment of the possible role(s) that the military could endorse to become active stakeholders in the planning and management of day-to-day manned aircraft and drone operations in U-space. As U-space relies on a highly automated and digitalised environment, this active role in managing U-space would require the exchange of operational data between military systems and U-space systems. Considering the sensitivity of military data and the need for investments on the military side, the goal of SC4 is thus to define several options for the active involvement of the military in U-space and compare them in terms of human, technology, financial, legal and operational impact and benefits.

Note 1: "Controlled airspace" is a generic term that covers the different classification of airspace (Class A, Class B, Class C, Class D, and Class E airspace) and defined dimensions within which air traffic control service is provided to IFR flights and to VFR flights in accordance with the airspace classification. Because of this definition, drone traffic in U-space could be considered as under some form of control service because of the mandatory use of U-space services and hence, U-space airspace could be considered as some form of controlled airspace, from a drone operations perspective.

To prevent any confusion, in this document, "controlled/uncontrolled airspace" should always be understood from a manned aviation perspective, i.e. referring to airspace classes where ATC service is provided to manned flights. Consequently, a U-space airspace designated in Class G airspace will be considered as uncontrolled airspace.

Note 2: using the above terminology, VFR flights in uncontrolled airspace can be provided with air traffic services in accordance with the airspace classification. This report assumes that military flights under VFR in uncontrolled airspace can be provided with the same services as civilian flights. This report also does not envisage IFR flights at very low level (except in the specific case of a CTR).

2.1 - U-space development

The development of U-space is essentially led by civilian entities and the "Military and U-space: guidelines" study conducted by EDA contributes to ensuring that military needs and constraints are properly understood and addressed in this development. The regulatory framework supporting the implementation of U-space is coming closer to completion and introduces significant changes to the way air traffic is currently managed by defining new types of airspace and new actors in charge of delivering services to airspace users in these areas. It is recognised that U-space is a new structure, which will impact both VFR GAT and OAT flights, e.g., in terms of aeronautical information and services.

2.1.1 - U-space at a glance

U-space is a set of new services relying on a high level of digitalisation and automation of functions and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. As such, U-space is an enabling framework designed to facilitate any kind of routine drone mission, in all classes of airspace and all types of environment - even the most congested - while addressing an appropriate interface with manned aviation and air traffic control.

U-space facilitates any kind of operations[1] for both, private and public drone users (including commercial and leisure users as well as State (including military) and public entities with appropriate prioritisation for special missions) *"in all operating environments[2], and in all types of airspace (in particular but not limited to very low level airspace[3])"* ([4]) by *"enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, ATM/ANS service providers and authorities."* ([4]).

The definition of U-space has been initiated by SESAR which proposed a definition of the new services brought by U-space as well as a concept of operations applicable to European airspace. Based on this work and through cooperation with aviation stakeholders, EASA has defined the regulatory framework in IR (EU) 2021/664, 2021/665 and 2021/666, that details the requirements around U-space – a set of new services and specific procedures designed to support safe, efficient, and secure access to airspace for large numbers of drones. This regulation enters into force on 26 January 2023 and introduces some important new features:

- **A new type of airspace**: a UAS geographical zone (as defined in IR (EU) 2019/947) can be designated by States as U-space airspace, where drones will only be able to operate if they use specific services.
- **A new set of services** for drone operators: in a given U-space airspace, drone operators will be required to use at least 4 mandatory services, and at the discretion of each State, up to 2 additional services. Those services are:
  - Geo-awareness - providing drone operators with the information about the latest airspace constraints and information on UAS geographical zones.
  - UAS flight authorisation - ensuring that authorised drone operations are free of intersection in space and time with any other notified drone flight authorisation within the same portion of U-space airspace.
  - Network identification - providing the identity of drone operators, the location and flight vector of drones, and sharing relevant information with other U-space airspace users.
  - Traffic information service - alerting drone operators about other air traffic that may be present in proximity to their drone.
  - Conformance monitoring (optional) - providing real-time alerting of non-conformance with the granted flight authorisation and informing the drone operators when they deviate from it.
  - Weather information (optional) - providing the drone operator with weather forecasts and actual weather information either before or during the flight.
- **New actors**: U-space Service Providers (USSPs) will be responsible for delivering the above services to drone operators. USSPs will rely on Common Information Services (CIS) to access some of the elementary data required to build the U-space services (cf. IR (EU) 2021/664 and its AMC/GM for details on this data). According to Article 5, paragraph 6 of Commission Implementing Regulation (EU) 2021/664, Member States have the option to designate a single common information service provider exclusively for supplying common information services within U-space airspaces under their responsibility. The use of "may" indicates that this designation is not mandatory or compulsory. This provision grants Member States the discretion to decide whether or not to designate a single provider for these services. If they choose to do so, the designated provider is obligated to distribute this information in accordance with Article 5, paragraph 5 of the same regulation.

  The present SC4 Final Report considers high-level U-space architectures both with and without a CISP designated (resp. centralised architecture and distributed architecture), reflecting the flexibility provided by the regulation to Member States in determining their approach to U-space implementation.

[1] Including visual line of sight (VLOS) and beyond visual line of sight (BVLOS) operations

[2] Urban, suburban, rural, regardless the density of population

[3] Very low level airspace refers to the airspace below 500ft

This new framework is illustrated by the following figure:

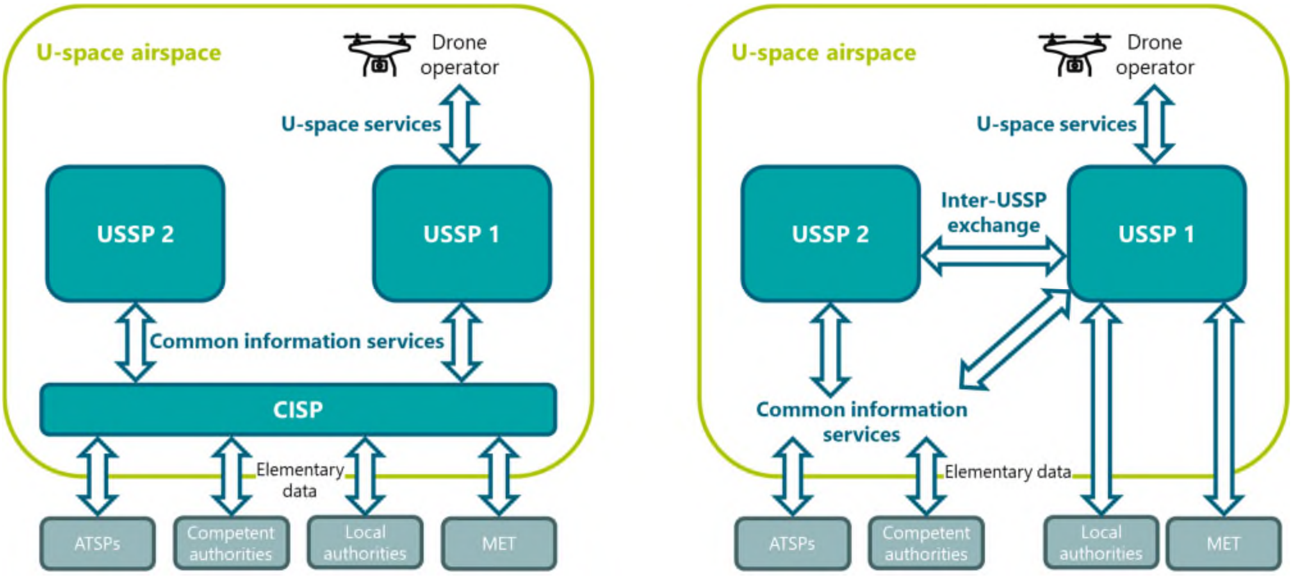


FIGURE 2: KEY FEATURES OF U-SPACE (LEFT: CENTRALISED ARCHITECTURE, RIGHT: DISTRIBUTED ARCHITECTURE)

At its core, U-space uses the principle of segregation between manned and unmanned traffic to ensure that the risk of collision between manned aircraft and drones is adequately mitigated. When a manned aircraft operates in U-space, it is required to be conspicuous to USSPs in that airspace, which can then inform drone operators about this traffic through the Traffic Information U-space service and take appropriate tactical measures (e.g. airspace restrictions, cancellation of flight authorisations) to ensure they are segregated. As for air traffic control before, it can be expected that USSPs will use data contained in the Traffic Information U-space service to extrapolate manned aircraft trajectories or feed sophisticated Conformance Monitoring algorithms that warn human actors and systems of impending hazardous situations or deviations before they actually occur.

In controlled airspace[4], ANSPs are also able to initiate a dynamic reconfiguration of the airspace to coordinate airspace restrictions with the USSPs, although this mechanism is expected by EASA to be used exceptionally as airspace design should be the primary means of maintaining the segregation between manned and unmanned traffic.

2.1.2 - Current state of U-space development

Following the publication of the European Commission's Drone Strategy 2.0 in November 2022, the publication of the AMC/GM for the U-space regulatory package in December 2022 and the entry into force of the U-space regulatory package in January 2023, the on-going implementation U-space has accelerated in 2023. In 2024, the SJU (SESAR Joint Undertaking) is working on the Air Traffic Management (ATM) Master plan[5] update which will include the U-space 2.0 which already considers a number of challenges that have emerged since it was initially defined in 2019.

Many EU Member States are actively working towards implementing U-space through the publication of national strategies and roadmaps, the transcription of EU regulation into national law, the designation of ANSPs as single CISP for all the U-space airspaces in the country and the definition of the processes that will allow certifying the future CISPs and USSPs. Implementation projects sponsored either by European institutions (e.g. SESAR 3 JU) or individual Member States continue to be launched to help stakeholders progress in the common

[4] *Cf. Note 1 in section 2 - Introduction, page 9*

[5] *The 2020 edition is the latest version of the ATM Master Plan*

understanding of U-space and to increase the maturity operational concepts, processes and technological solutions.

In parallel, some MS are also preparing the designation of U-space airspaces, by identifying these airspaces and defining the processes and means to issue the corresponding information to interested stakeholders.

Those ANSPs that have already been designated at CISPs, or will be soon, are defining the systems that will allow them to collect elementary data from the various sources and provide the CIS to USSPs and other interested U-space stakeholders. In parallel, they are also adapting their organisation to their new responsibilities and preparing the associated certification processes with their civil aviation authority. There are three possible organisational models that Member States could decide to adopt (in the case where a single CISP is designated by the MS) when implementing the new roles required by U-space:

- **Model A:** The CISP and USSP are two entities (or they are a single entity) separate from the national civilian ANSP.
- **Model B:** The CISP entity is part of the national civilian ANSP organisation, while the USSP is created as an external entity.
- **Model C:** The CISP and USSP are created as new departments within the current organisation of the national civilian ANSP.

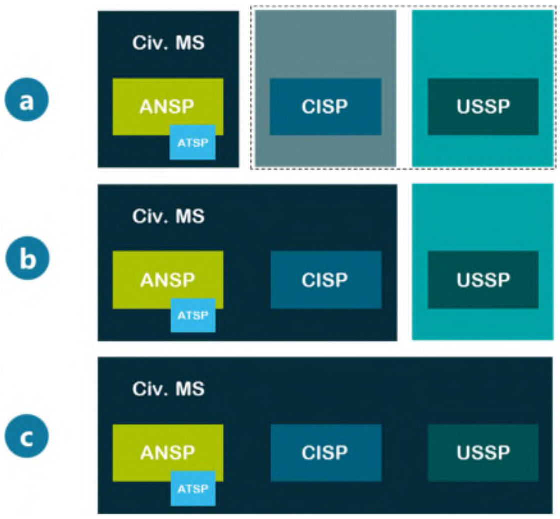


FIGURE 3: POSSIBLE CIVILIAN U-SPACE ORGANISATIONAL MODELS

Depending on the approach that the military would use for playing an active role in U-space, they may have to implement a coordination process and exchange information with several entities. Therefore, the local organisation adopted by civilian U-space stakeholders will have a significant impact on the military.

<u>Note:</u> for simplicity's sake; the present report assumes that:

- the single CISP, when one is designated, is a new department within the national civilian ANSP's organisation;
- USSPs are distinct from the national civilian ANSP (i.e. model B above).

This approach has indeed been adopted by those MS that are most advanced in the implementation of U-space even though models A and C in Figure 3 are also allowed by the U-space regulatory framework. The limited number of MS having adopted a distributed U-space architecture makes it difficult to suggest a generic organisational model in this case and the ANSP has less responsibilities in the management of U-space.

The current state of civil-military cooperation in the context of U-space is characterised by strong emphasis on coordination and collaboration, as stated in the European Commission's Drone Strategy 2.0. In line with this strategy, Eurocontrol is leading an effort in addressing key defence and technological issues within military aviation, particularly in light of the Russian invasion of Ukraine.

Eurocontrol underscores the importance of civil-military coordination to avoid adverse impacts on national and collective defence capabilities. Moreover, the integration of military trajectory data, collaborative decision-making, and compliance with military GNSS receivers for State aircraft operations in a Performance-Based Navigation (PBN) environment are among the key technological topics currently discussed. These discussions also extend to the emerging civil-military interface required by U-space, indicating a proactive approach towards ensuring that the integration of urban air taxis, drones, and other U-space users does not compromise security, defence, and safety[6].

2.1.3 - The safety challenges for the military

The introduction of new airspace users and the evolving airspace dynamics present safety challenges for military operations, as they often take place in uncontrolled, low-level airspace where U-space is expected to be active. Without access to the Dynamic Airspace Reservation (DAR) system and lacking ADS-B equipage, military traffic may be difficult to separate from drone operations.

The military need to identify additional means to e-conspicuity and DAR to ensure that they can operate safely in U-space airspace, notably when it is designated in uncontrolled airspace.

The previous SC3 proposed solutions to mitigate these risks. The key prerequisite is real-time information exchange between military and U-space entities. This enables the safe conduct of operational or emergency military flights, which may not follow pre-planned routes. Implementing systems that allow for instantaneous sharing of information in the strategic, pre-tactical and tactical phases of operations would significantly reduce the risk of conflicts between civilian drones and military assets.

Furthermore, the development of interoperable technologies that bridge the gap between military specifications and U-space requirements will be essential. Establishing protocols for emergency communication and rapid response mechanisms will further ensure that unplanned military activities can integrate seamlessly into the U-space without compromising safety. Additionally, conducting joint exercises and simulations could help both military and civilian airspace users to better understand each other's operational paradigms, enhancing overall safety within the shared airspace.

Lastly, a collaborative approach in policy-making and technical standardisation can facilitate a unified airspace environment that accommodates the unique needs of military operations while advancing U-space objectives.

2.2 - On this report

The present report documents a detailed assessment of the possible role(s) that the military could endorse to become active stakeholders in the planning and management of day-to-day manned aircraft and drone operations in U-space. This assessment develops a detailed description of each of the scenarios, notably looking at factors such as regulation, governance, technology, operational processes and financing. In order to identify the potential and risks associated with each scenario, a comparative analysis of the selected scenarios was carried out using a set of evaluation criteria. The assessment was conducted using a SWOT (Strength, Weakness, Opportunity, Threat) approach, a methodology which allowed highlighting the strengths and weaknesses of each of scenario.

The proposed scenarios intend to rely on existing infrastructure, procedures, principles and systems to a maximum extent possible in order to minimise the impact on the military. The following list provides the main ATM and U-space principles that could benefit military operations in U-space:

- **Collaborative Information Sharing** about airspace and traffic, facilitating a comprehensive awareness of civilian and other military operations.
- **Flexible Use of Airspace (FUA)**, which allows for the dynamic allocation of airspace based on current needs rather than fixed structures, could be adapted to enhance military operational flexibility and

[6] *https://www.eurocontrol.int/news/31st-eurocontrol-military-atm-board-examines-key-defence-and-technological-issues-facing*

efficiency, ensuring that airspace is used in the most optimal way to accommodate both civilian and military needs efficiently.

- **Geofencing** provides a way to define virtual boundaries for drone operations, which can be adapted to restrict UAVs from entering sensitive military zones.
- **Traffic Information Services** offer real-time data on airborne traffic, which can enhance situational awareness and prevent potential conflicts between military and civilian airspace users.
- **Priority Services** could ensure that military flights have the necessary priority in airspace management, especially during critical operations.
- **Strategic Deconfliction** involves planning and managing airspace use in advance to prevent potential conflicts, enhancing the safety and efficiency of both military and civilian flights.

2.3 - Document structure

This report is composed of the following 8 main sections:

SECTION 1 - EXECUTIVE SUMMARY that brings a condensed and clear outline of the SC3 report.

SECTION 2 - INTRODUCTION is intended to provide a detailed presentation of the report, its objectives and the approach undertaken.

SECTION 3 - APPROACH TO describes the methodology adopted to conduct the analysis summarised in the present report.

SECTION 4 - POSSIBLE ROLES FOR THE MILITARY IN U-SPACE defines a number of roles that the military could adopt in U-space and compares them, using a single set of pre-defined criteria, leading to the selection of one or several preferred operational scenarios that are assessed in detail in the following sections.

SECTION 5 - SUPPORTING ORGANISATION FOR OPERATIONAL SCENARIO(S) details the business models that would enable a military organisation to use and/or provide services in a U-space environment, according to the operational scenarios selected in the previous section.

SECTION 6 - ASSESSMENT OF IMPACT ON MILITARY SYSTEM INTERFACES assesses the impact on military systems of implementing exchange of information with U-space, as a consequence of the various operational scenarios under consideration.

SECTION 7 - FINANCIAL ASSESSMENT provides an assessment of the costs that the military would accrue to implement the concept proposed in the previous section.

SECTION 8 - GUIDELINES ON A FUTURE ROLE FOR THE MILITARY IN U-SPACE concludes on the work presented in the report.

This report is complemented by two annexes providing a definition of the terms used in the document and a list of key reference documents.

3 - APPROACH TO SC4 ASSESSMENT

The key objective was to perform a detailed assessment of the possible role(s) that the military could endorse to become active stakeholders in the planning and management of day-to-day manned aircraft and drone operations in U-space. As U-space relies on a highly automated and digitalised environment, this active role in managing U-space would require the exchange of operational data between military systems and (civilian) U-space systems. Considering the sensitivity of military data and the need for investments on the military side, the goal is to define several options for the active involvement of the military in U-space and compare them in terms of human, technology, financial, legal and operational impact and benefits.

The initial stage involved outlining five operational scenarios that describe potential military roles within the U-space environment. The scenarios are described in more detail in section 4.1 -

To support a fair comparison of the different options available to the military, SC4 defined a set of assessment criteria. A multi-criteria analysis approach ensured a thorough and systematic evaluation of the different operational scenarios related to the military's possible role in U-space. By considering a wide range of criteria, SC4 investigates all aspects of the selected scenarios. The aim is to identify the most appropriate scenario(s), taking into account the governance, regulatory, operational, technical, financial and manpower aspects, thus ensuring well-informed guidelines.

To identify the potential and risks associated with each scenario, a comparative analysis of these agreed scenarios was performed using the same set of assessment criteria. Initially, a comprehensive assessment of the impact, strengths, weaknesses, and trade-offs associated with each scenario across the defined criteria was conducted. Subsequently, a SWOT (Strengths, Weaknesses, Opportunities, Threats) approach was employed, leading to the identification of one or several preferred business models that offered the best chances for the military to benefit from the U-space opportunities while remaining resilient to the uncertainties and risks associated with the development of U-space.

Moreover, several business models that would enable a military organisation to use and/or provide services in a U-space environment were developed. After considering the main functions currently ensured by this organization, an analysis was conducted to assess how a new role associated with U-space would fit within this organization. The goal was to identify whether commonalities and synergies could be found to reduce the impacts of implementing this new role on humans, systems, and operational processes.

Given the similarities in the functions ensured by the military ANSPs with their civilian counterparts, and because civilian ANSPs in several MS were currently adapting their organisation to their future role in U-space, an understanding of how these civilian ANSPs are addressing these transformation projects and which business models they are aiming to adopt provided valuable insights for the end results of this report. This benchmarking exercise provided possible setups for Common Information and U-space services provision.

The subsequent step involved identifying the interoperability needs for exchanging information between military ATM/Air Defence (AD) systems and U-space systems. This was done by utilizing stakeholder requirements, system requirements, and relevant standards and regulations as a framework for eliciting these needs. The outcome was a comprehensive set of requirements that captured known factors and allowed for future updates.

During this phase, the technical architecture for military ATM/AD and U-space systems, along with their interfaces, was formally described. Major components and functions were outlined, providing a generic yet sufficient description for assessing the impacts of military involvement in U-space. The result was a diagram or series of diagrams illustrating the systems and interfaces for different operational scenarios.

Based on the previous findings, necessary changes to military ATM/AD systems to support various considered roles were identified. This involved describing modifications to existing systems and interfaces and identifying needs for new systems and interfaces. The outcome was an analysis of the technical changes required for each operational scenario.

Further steps involved conducting a financial analysis of the different scenarios under consideration. This analysis primarily relied on the monetization of costs, specifically the investments in CAPEX and OPEX required for the military to implement their new roles, as it was anticipated that financial benefits would be limited due to the potential for reducing current expenditures or generating additional revenues appearing limited at best. To accomplish this, assumptions regarding costs and benefits were established based on the services' value chains and the mechanisms for costs and benefits defined in previous tasks and Specific Contracts. The results of the financial analysis were presented through various indicators, including the cumulative discounted benefits and costs, the Net Present Value, the Return-on-Investment Ratio, and the payback period.

Finally, based on the comprehensive analysis and findings derived from the various tasks conducted, recommendations were formulated for the military. These recommendations encompass strategic directions, operational adjustments, and potential investments to optimise the implementation of new roles and enhance overall effectiveness. The insights gained from the analysis served as a foundation for developing actionable strategies aimed at improving interoperability, resource allocation, and decision-making processes within the military framework. Moreover, these recommendations were tailored to address specific challenges identified during the analysis while capitalising on emerging opportunities in the evolving landscape of military air operations and U-space integration.

4 - POSSIBLE ROLES FOR THE MILITARY IN U-SPACE

4.1 - Operational scenarios for military involvement in U-space

4.1.1 - Introduction

This sub-section introduces the key principles of the U-space such as geographical zones or Dynamic Airspace Reconfiguration (DAR). The main part of this section then introduces five scenarios assessing the impact of U-space on the Military. The following scenarios for Military were considered:

- **Scenario 0:** UAS geographical zone manager;
- **Scenario 1:** consumer of U-space services;
- **Scenario 2:** consumer and provider of information to CIS;
- **Scenario 3:** national military USSP;
- **Scenario 4:** pan-European military USSP.

4.1.1.1 - The need for geographical zones

At strategic airspace management level, the military authorities designate HTA (Helicopter Training Areas) and LFA (Low Flying Areas) to enable flights of fighter jets, transport aircraft or a mixed training forces) within uncontrolled airspace (Class G) from ground up to 500 feet. These areas shall be determined by lateral and vertical boundaries, with regulated status (e.g. R or D) and published in the national Aeronautical Information Publication (AIP) or through Notices to Airmen (NOTAMs). The UAS geographical areas that provide drone operators with the information about the airspace constraints shall be established as part of the U-space to protect the HTA and LFA against conflicts with unmanned traffic.[7]

4.1.1.2 - Dynamic Airspace Reconfiguration (DAR)

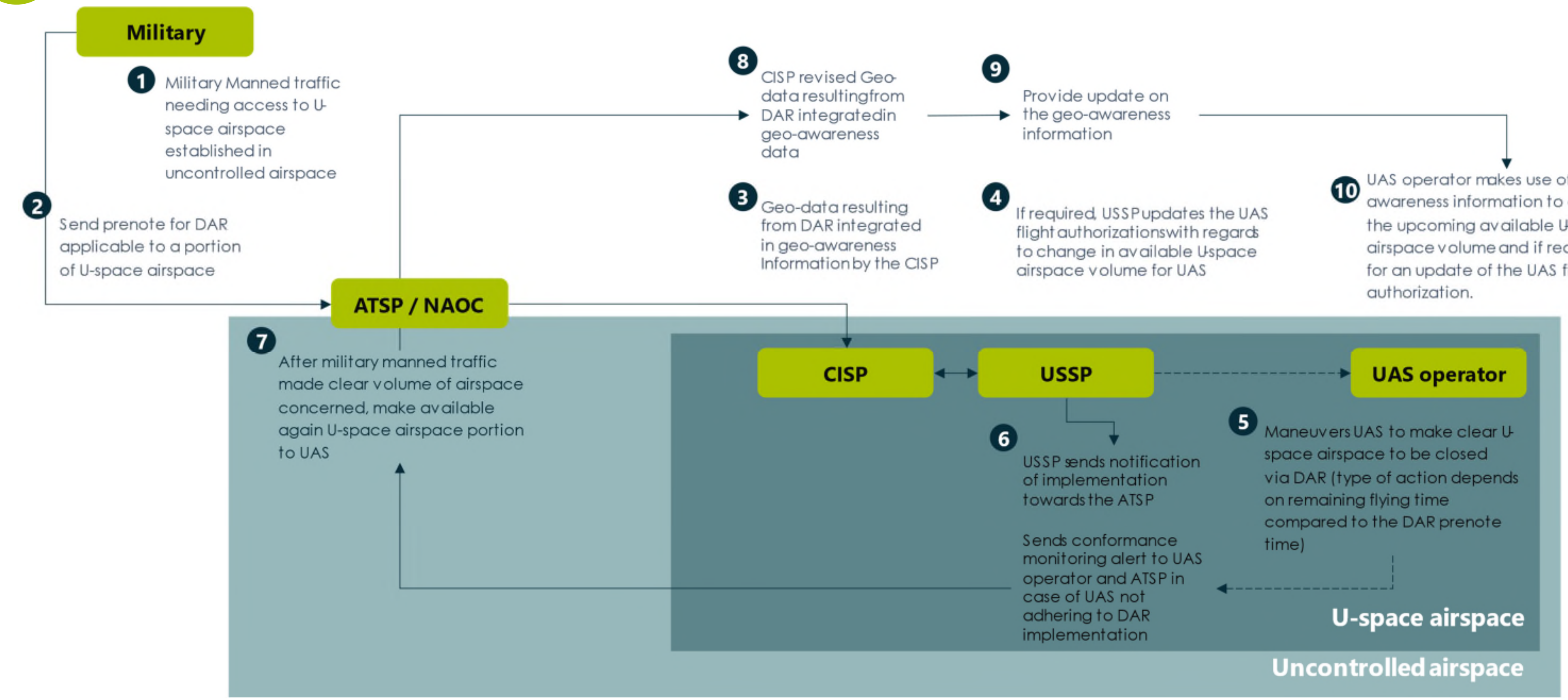
Implementing Regulation (EU) 2021/665 requires ATSPs to conduct a so-called dynamic reconfiguration of the U-space airspace, when within controlled airspace, to ensure that manned and unmanned aircraft remain safely segregated. This is achieved through coordination between the ATSP responsible for the provision of air navigation services in this airspace and the USSP(s) operating in this specific U-space airspace.

SC3 ([8]) has already suggested to extend this coordination mechanism to any type of U-space airspace, whether it is designated in controller or uncontrolled airspace, as a additional layer of safety for military aircraft that cannot be conspicuous to USSPs or which operations cannot be planned in advance (e.g. emergency medical evacuation, firefighting, air policing, SAR, etc.). A military ATS unit (ATSU) or controlling unit (CRC) should be able to accommodate a short-term change of demand in capacity for military manned aviation, or in case of emergency. In this case, it would be the responsibility of the (civilian or military) controller to perform the DAR, taking into account the prenote time between the announcement of the change and the activation of the change. From the moment the U-space airspace is again available to unmanned aviation, it would be the controller's responsibility to inform manned traffic to not enter the U-space airspace volume. In uncontrolled airspace, SC3 suggested that the NAOC acted as the interface between military ATSUs/CRCs and USSPs for requesting and implementing short-term U-space airspace adaptations.

By default, this proposed approach implies that only few changes to the DAR process detailed in the U-space regulation are to be expected. The U-space airspace could be subdivided into portions (cf. AMC/GM [6] – GM1 to Article 4, item d) in order to offer flexibility in the management of this airspace and not to unnecessarily impact U-space capacity.

It is to be understood that when temporarily limiting the available U-space airspace, this part of the U-space airspace that becomes unavailable to drone operations is not disappearing. This only means the USSP is not allowed to grant UAS flight authorisations and instructs on-going operations to vacate that part of the U-space airspace or land, from the moment the reconfiguration comes into force. Rejecting or revising a UAS flight authorisation is the responsibility of the USSP providing services to UAS operators.

[7] *In some cases, the whole FIR can be classified as HTA (e.g. Germany).*



1 Military Manned traffic needing access to U-space airspace established in uncontrolled airspace

2 Send prenote for DAR applicable to a portion of U-space airspace

3 Geo-data resulting from DAR integrated in geo-awareness Informationby the CISP

4 If required, USSPupdates the UAS flight authorizationswith regards to change in available Uspace airspace volume for UAS

5 Maneuvers UAS to make clear U-space airspace to be closed via DAR (type of action depends on remaining flying time compared to the DAR prenote time)

6 USSP sends notification of implementation towards the ATSP

Sends conformance monitoring alert to UAS operator and ATSP in case of UAS not adhering to DAR implementation

7 After military manned traffic made clear volume of airspace concerned, make available again U-space airspace portion to UAS

8 CISP revised Geo-data resultingfrom DAR integratedin geo-awareness data

9 Provide update on the geo-awareness information

10 UAS operator makes use of the geo-awareness information to evaluate the upcoming available Uspace airspace volume and if required file for an update of the UAS flight authorization.

FIGURE 4: SUGGESTED DAR PROCESS FOR U-SPACE IN UNCONTROLLED AIRSPACE

4.1.2 - Scenario 0: UAS geographical zone manager

Geo-awareness information is based on a collection of data (part of which can originate from the military) provided by the CISP to the USSPs and intended to be used both by the USSP itself and by UAS operators. The USSP will use it for the UAS flight authorisation service as a source of data to inform UAS operators of relevant operational constraints and changes both prior to and during the flight. The operator will use it as part of the pilot's responsibility to take due consideration to the geo-awareness data in a timely manner when operating the UAS.

A dynamic airspace reconfiguration (DAR) will result in an update to the geographical data describing the U-space airspace and shall be treated by UAS operators in the same way as a no-drone zone. This updated geographical data shall be made available to USSPs through the CIS. The USSP shall take this change into account for UAS flight authorisations and shall request UAS operator already flying in the deactivated portion of the U-space airspace to act accordingly.

The figure below shows the communication links and data flows when the military would be involved in the provision of geo-awareness information.

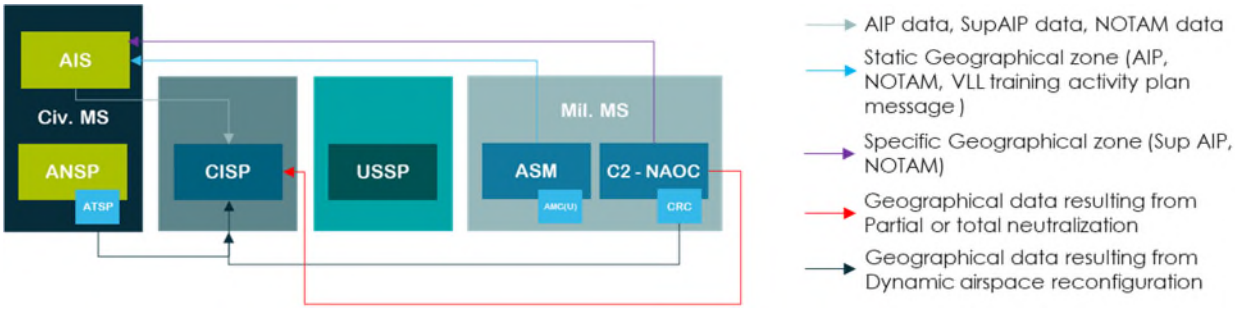

AIS
Civ. MS
ANSP
ATSP
CISP
USSP
Mil. MS
ASM
AMC(U)
C2 - NAOC
CRC
AIP data, SupAIP data, NOTAM data
Static Geographical zone (AIP, NOTAM, VLL training activity plan message)
Specific Geographical zone (Sup AIP, NOTAM)
Geographical data resulting from Partial or total neutralization
Geographical data resulting from Dynamic airspace reconfiguration

FIGURE 5: INFORMATION FLOWS FOR GEO-AWARENESS (SCENARIO 0)

A section of the national Airspace Management Cell dedicated to uncontrolled U-space airspace (AMC[U]) could act as pre-tactical manager, by managing and disseminating information/data to the CISP/CIS. This includes day-to-day activation periods of UAS geographical areas by NOTAM and VLL training activities. (cf. D1, D2, D3 & SC3)

4.1.2.1 - Impact of the scenario

The scenario 0 implies only a few changes to the current U-space architecture. The U-space airspace may be divided into UAS sub-geographical zones (cf. SC3) in order to limit capacity decrease when military assets transit through U-space airspaces.

A systemic coordination between the NAOC, ATS and Military Controlling units on the one hande, and the CISP/USSP on the other hand would allow for the generation and sharing of geographical data resulting from DAR.

It should be noted that in such events, the USSP is not allowed to grant UAS flight authorisations inside the concerned airspace, and instructs ongoing operations to vacate the airspace as from the moment the limitation comes into force. In this context, the USSP is responsible for rejecting and/or revising a UAS flight authorisation.

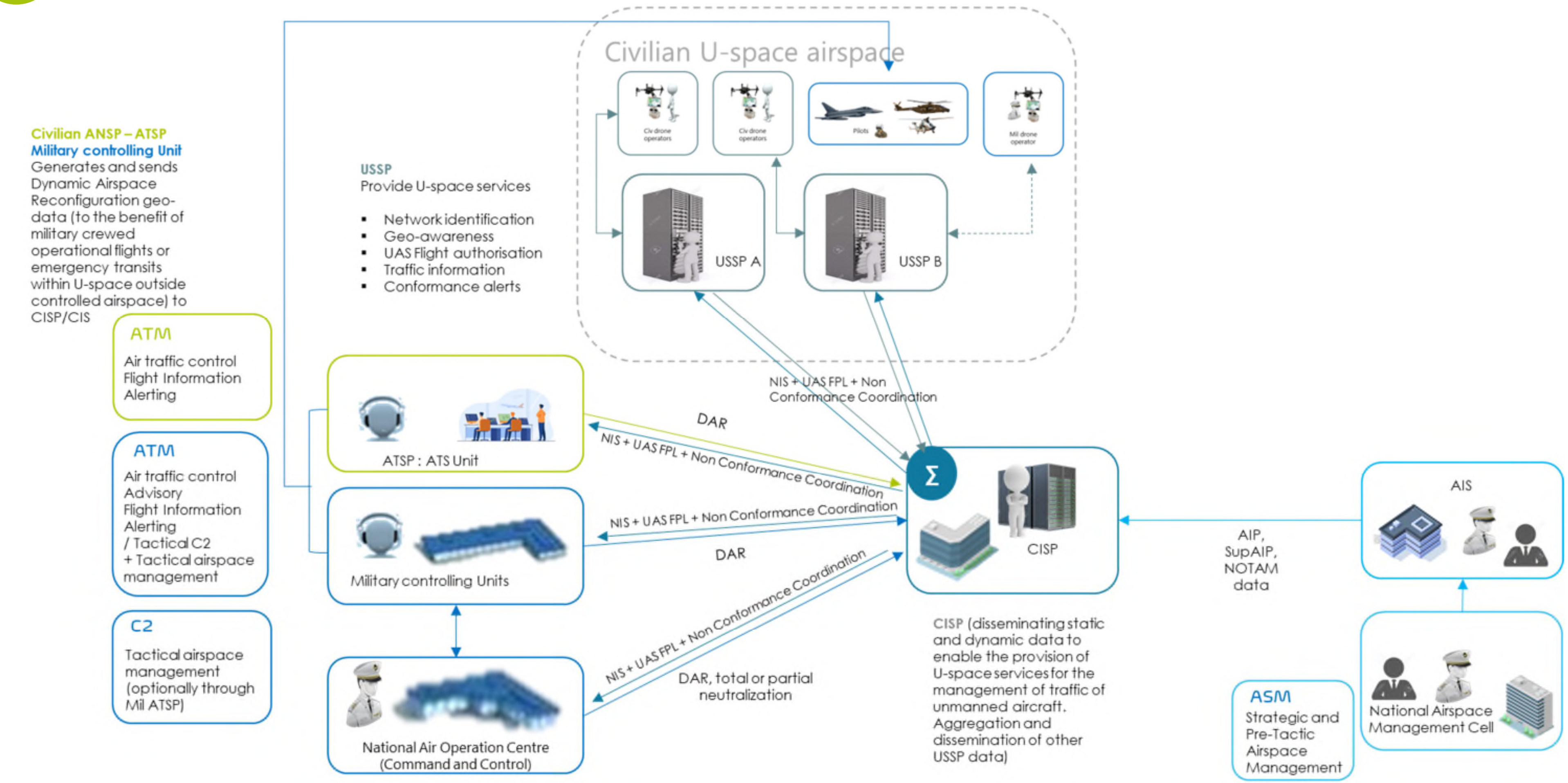
> Note: The USSP role considered in all scenarios assumes that the military USSP is able to support unmanned flights coordination in the strategic and pre-tactical phases. A UTM capability would have to be set up to allow coordination in the tactical phase of operations in controlled airspace. This study also proposed a light, low-cost coordination solution for uncontrolled airspace that does not require the military to implement UTM capability (cf. SC3 Final Report [8], section 4.3).

4.1.3 - Scenario 1: consumer of U-space services

The Scenario 1 envisages that the military become a consumer of U-space services. The Member State's choice of the U-space architecture (see 2.1.1 -) has no impact on the operational benefits that the services of the U-space ecosystem would bring to the military. In this scenario, the military would retain the responsibilities of UAS geographical zone manager as described in Scenario 0.

4.1.3.1 - Impact of the scenario

The data exchanges between the military stakeholders (ASM/NAOC) remain unchanged regardless of the model and have no impact on the operational benefits to the military.


Civilian U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
USSP A
USSP B
NIS + UAS FPL + Non Conformance Coordination
DAR
NIS + UAS FPL + Non Conformance Coordination
NIS + UAS FPL + Non Conformance Coordination
DAR
NIS + UAS FPL + Non Conformance Coordination
DAR, total or partial neutralization
ATSP : ATS Unit
Military controlling Units
National Air Operation Centre (Command and Control)
Σ
CISP
AIS
AIP, SupAIP, NOTAM data
National Airspace Management Cell

Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS

USSP
Provide U-space services

- Network identification
- Geo-awareness
- UAS Flight authorisation
- Traffic information
- Conformance alerts

ATM
Air traffic control
Flight Information
Alerting

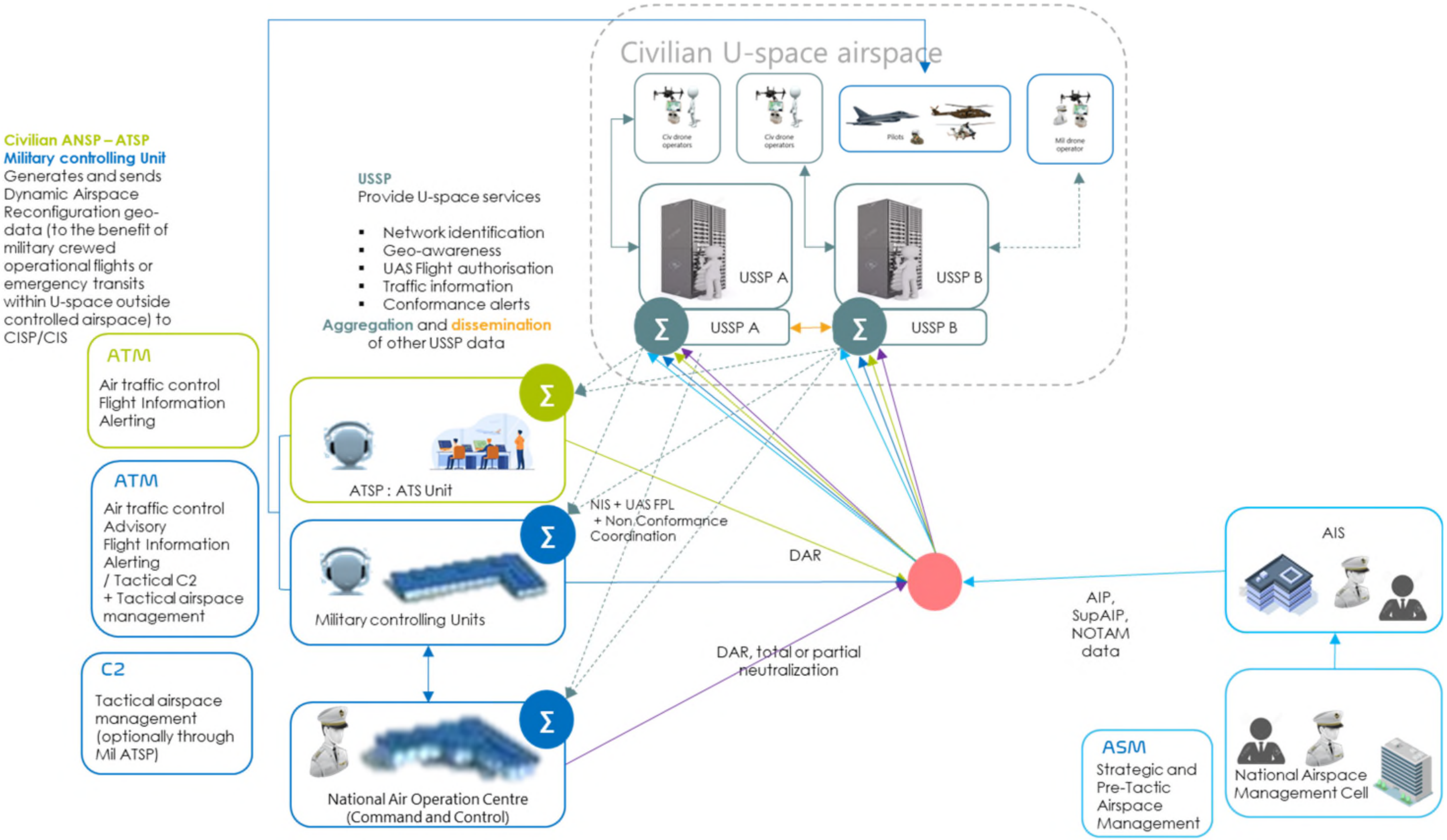
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management

C2
Tactical airspace management (optionally through Mil ATSP)

CISP (disseminating static and dynamic data to enable the provision of U-space services for the management of traffic of unmanned aircraft. Aggregation and dissemination of other USSP data)

ASM
Strategic and Pre-Tactic Airspace Management

FIGURE 6: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 1) – CENTRALISED MODEL (SINGLE CISP)



Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS

USSP
Provide U-space services

- Network identification
- Geo-awareness
- UAS Flight authorisation
- Traffic information
- Conformance alerts

Aggregation and dissemination of other USSP data

Civilian U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
USSP A
USSP B
Σ USSP A
Σ USSP B
ATM
Air traffic control
Flight Information
Alerting
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management
C2
Tactical airspace management (optionally through Mil ATSP)
Σ
ATSP : ATS Unit
Σ
Military controlling Units
Σ
National Air Operation Centre (Command and Control)
NIS + UAS FPL
+ Non Conformance Coordination
DAR
DAR, total or partial neutralization
AIP, SupAIP, NOTAM data
AIS
ASM
Strategic and Pre-Tactic Airspace Management
National Airspace Management Cell

FIGURE 7: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 1) – DISTRIBUTED MODEL (NO CISP)

SC4 identified three U-space services potentially having an impact on the Military as part of the U-space – Network Identification, UAS flight authorisation and Conformance monitoring.

Network Identification Service (NIS) – The network identification service has a dual purpose:

- It enables USSPs to each acquire the real-time position data of the airborne UAS of their own customers.
- It allows sharing this real-time position data with the single CISP. The CISP system acts as a data broker platform involved not only in collecting the NIS data from all USSPs, but also in the aggregation and dissemination of the NIS data (collected by each of the USSPs from its respective customers). Aggregated NIS data should be used as an input to the USSPs traffic information service.

The NIS can support the Military with:

- **Increased Mission Effectiveness:** By using cooperative drone identification and position sharing through the network information service, Air Surveillance Operators would be able to detect, track, and identify drones in the U-space airspace, enhancing the UAS RAP (Recognized Air Picture).
- **Improved Safety:** Tactical Controllers would be aware of drone flights when supporting air operations, thereby ensuring safety for those flights.
- **Enhanced Network Information Service Utility:** The NAOC/Military Controlling Units must be connected to the CISP/USSP and able to analyse, integrate, and display NIS data. Although this can be achieved via a separate network/display, it might result in additional costs.

The following points need to be considered in order to materialise the benefits mentioned above:

- **Additional Costs and Cyber Security Risks:** Adapting and maintaining military systems to use this service could lead to more expenses and the emerging needs to manage new cyber security risks.
- **Safety Management System Needs:** The use of this service might require the definition and implementation of new controls within a Safety Management System (SMS).
- **Training Requirements:** Air Surveillance Operators and Tactical Controllers would need additional training to understand and use the information provided by the network information service.

UAS flight authorisation service – the flight authorisation service consists of UAS operators submitting flight authorisation requests to USSPs. The USSPs issue the flight authorisation only if the requested flight is free of conflict with any other notified UAS flight authorisations within the same U-space airspace. The USSP shall coordinate/communicate issuing of the flight authorisation with other USSPs within the U-space while also considering the manned/unmanned traffic information and geo-awareness information. The flight authorisation service can support the Military with:

- **Increased Mission Effectiveness:** The exchange of flight plan information through the service could improve the UAS RAP allowing Air Surveillance Operators to correlate drone tracks to flight authorisations, thereby more easily identifying drone flights .
- **Improved Safety:** Tactical Controllers will have greater awareness of the path and intent of drone pilots enhancing safety during air operations that they are responsible for overseeing.
- **Dynamic Reconfiguration:** In cases where there is a need to temporarily restrict the U-space airspace, the Tactical Controller can ensure that the space is monitored for drone traffic, thereby enforcing a safer operational environment.

The following points need to be considered in order to materialise the benefits mentioned above:

- **Training Needs:** Air Surveillance Operators and Tactical Controllers would require additional training to effectively utilise the information provided by the UAS flight authorisation service.
- **Cyber Security and Additional Costs:** Utilising the UAS flight authorisation service may result in additional costs for adapting and maintaining military systems. Moreover, integrating information from

CISP systems introduces an additional cyber security risk, necessitating the establishment of appropriate controls and a potential safety management system.

Conformance monitoring service – The conformance monitoring service can be viewed from two angles. Firstly from USSP-UAS operators coordination and secondly from an ecosystem-wide coordination. The USSP-UAS operator conformance coordination consists of the USSP continuously monitoring UAS operator's adherence to the authorised flight plan. The wider conformance monitoring ensures coordination between UAS', USSPs withing the same U-space airspace and ATSP in the event of UAS deviating from the intended operations. The conformance monitoring service can support the Military with:

- **Increased Mission Effectiveness:** The service enables the exchange of non-conformance alerts, which can improve the UAS RAP. Air Surveillance Operators can use these alerts to improve awareness of drone behaviour, which is critical for the execution of air defence missions.
- **Improved Safety:** Tactical Controllers gain improved situational awareness with information on drone flight paths and intentions, which contributes to the safety of flights they control.
- **Dynamic Airspace Management:** In the event of needing to restrict the U-space airspace, the Tactical Controller would be able to monitor the airspace effectively to ensure no unauthorized drone traffic penetrates the restricted airspace.

The following points need to be considered in order to materialise the benefits mentioned above:

- **Training Requirements**: Both Air Surveillance Operators and Tactical Controllers would require additional training to interpret and use the information provided by the Conformance Monitoring Service.
- **Cyber Security and Additional Costs**: Implementation of the service might result in additional costs to adapt and maintain military systems. Furthermore, integration with CISP systems would raise cyber security risks, requiring the development of appropriate controls and potentially a safety management system.

4.1.4 - Scenario 2: consumer and provider of information to CIS

The Scenario 2 envisages that the military becomes a consumer and a provider of information from/to the CIS/CISP. The Member State's choice of the organisational model (A, B, C explained in Scenario 1 in section 4.1.3 -) has no impact on the operational benefits that the services of the U-space ecosystem would bring to the military. In this scenario, the military would:

- Retain the responsibilities of UAS geographical zone manager as described in Scenario 0.
- Retain benefits described as part of the Scenario 1 (consumer of U-space services, including CIS).
- Provide military-specific information to U-space via the CISP and consume CIS provided by the civil sector. The CIS data provided by the military could include positioning data of military aircraft operating/transiting in U-space airspace, thus compensating for the absence of e-conspicuity capabilities in an uncontrolled airspace.

Under this scenario 2, military drone operators could also benefit from U-space services, or similar services, provided by a dedicated military entity, which could improve the coordination between manned and unmanned military flights. This approach could also allow coordination between unmanned military flights and civilian traffic. The present report does not further explore the services that could be provided to military drone operators and the benefits they would accrue, as SC4 focuses on organisational and high-level architecture aspects.

4.1.4.1 - Impact of the scenario

This extra layer of positioning data increases the safety within the U-space as it enhances the traffic information service provided by the USSP.

The military controlling units should be able to coordinate/communicate with the CISP and have the ability to share and utilise operational manned traffic data (as outlined in the figure below). Establishing the interfaces and processes would likely generate significant costs to upgrade and maintain military systems. Furthermore, safety assessments could be requested by the regulators in order to comply with the Safety Management System (SMS).

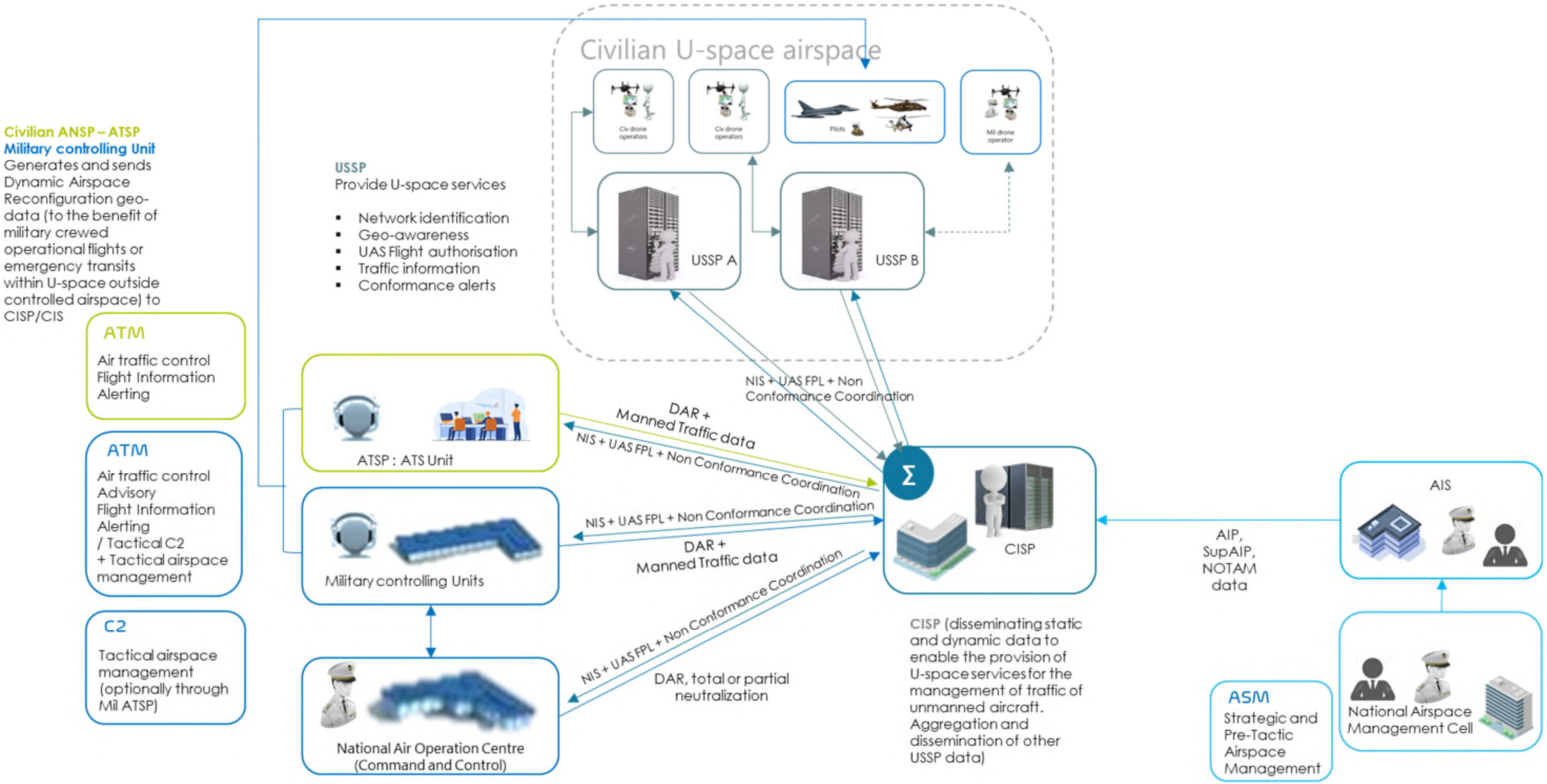

Civilian U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
USSP A
USSP B
USSP
Provide U-space services
▪ Network identification
▪ Geo-awareness
▪ UAS Flight authorisation
▪ Traffic information
▪ Conformance alerts
Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS
ATM
Air traffic control
Flight Information
Alerting
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management
C2
Tactical airspace management (optionally through Mil ATSP)
ATSP : ATS Unit
Military controlling Units
National Air Operation Centre (Command and Control)
NIS + UAS FPL + Non Conformance Coordination
DAR + Manned Traffic data
NIS + UAS FPL + Non Conformance Coordination
NIS + UAS FPL + Non Conformance Coordination
DAR + Manned Traffic data
NIS + UAS FPL + Non Conformance Coordination
DAR, total or partial neutralization
Σ
CISP
CISP (disseminating static and dynamic data to enable the provision of U-space services for the management of traffic of unmanned aircraft. Aggregation and dissemination of other USSP data)
AIP, SupAIP, NOTAM data
AIS
National Airspace Management Cell
ASM
Strategic and Pre-Tactic Airspace Management

FIGURE 8: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 2) – CENTRALISED MODEL (SINGLE CISP)

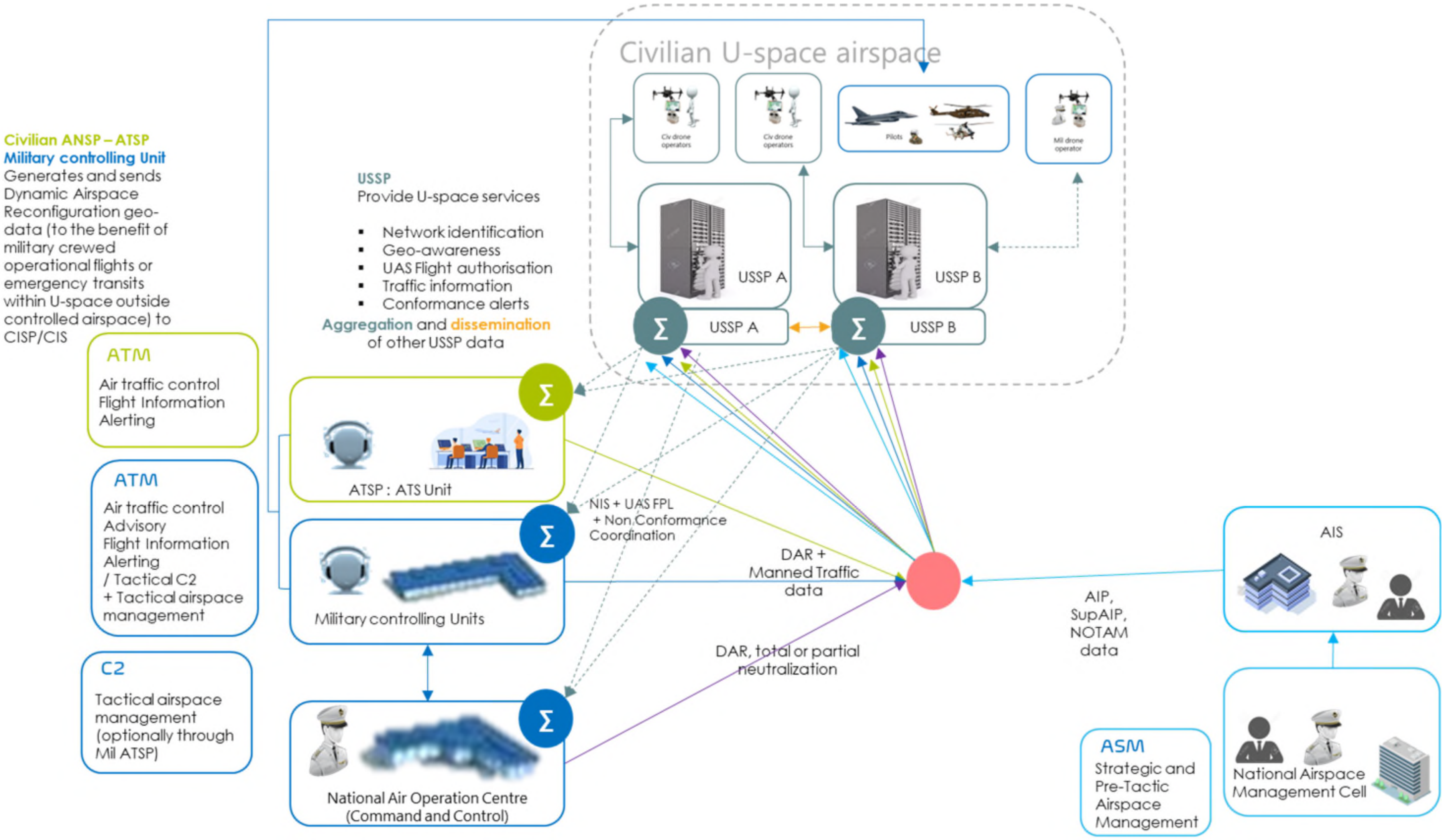

Civilian U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
USSP A
USSP B
Σ USSP A
Σ USSP B
Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS
USSP
Provide U-space services
▪ Network identification
▪ Geo-awareness
▪ UAS Flight authorisation
▪ Traffic information
▪ Conformance alerts
Aggregation and dissemination of other USSP data
ATM
Air traffic control
Flight Information
Alerting
ATSP : ATS Unit
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management
Military controlling Units
C2
Tactical airspace management (optionally through Mil ATSP)
National Air Operation Centre (Command and Control)
NIS + UAS FPL
+ Non Conformance Coordination
DAR +
Manned Traffic
data
DAR, total or partial neutralization
AIP,
SupAIP,
NOTAM
data
AIS
ASM
Strategic and Pre-Tactic Airspace Management
National Airspace Management Cell

FIGURE 9: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 2) – DISTRIBUTED MODEL (NO CISP)

4.1.5 - Scenario 3: national military USSP

The Scenario 3 envisages that the military becomes a national USSP. The Member State's choice of the organisational model (A, B, C mentioned explained within Scenario 1 in section 4.1.3) has no impact on the operational benefits that the services of the U-space ecosystem would bring to Military. In this scenario, the Military will:

- Retain the responsibilities of UAS geographical zone manager as described in Scenario 0.
- Retain benefits described as part of the Scenario 1 (consumer of U-space services).
- Share information about manned military aircraft within the U-space through CISP as part of Scenario 2 (provider of information to CISP)

The air force must have a certified system to assume the role of USSP in order to provide U-space services (5 mandatory and 2 optional) relying on digitalisation and automation of functions designed to support a safe, secure and efficient access to U-space airspace for a large number of UAS, especially considering U-space airspace configuration.

The benefits and risks related to this scenario will depend on the fact whether the U-space services will be provided to all UASs or to state drones (military, force protection, public services) only.

The military system for USS provision shall be able to:

- Acquire the real-time position data (with cooperative/acquisition data) of the airborne UAS controlled by the Military USSP.
- Share the acquired real-time position data with other stakeholders (eg CISP, USSPs, UAS operators) via sCISP (to be used as input to their traffic information service).
- Integrate the Network Identification Service data aggregated and disseminated by CISP (collected by each of the USSPs from its respective customers).
- Treat AIP data, NOTAM data and geographical data resulting from DAR distributed by CISP (UAS flight authorisation service) and disseminate (Geo-awareness service).
- Analyse UAS flight authorisation requests.
- Exchange issued flight authorisations between all USSPs via CISP.
- Share real-time positions of all the UAS' under Military USSP's control with other USSPs and authorised users.
- Ensure it is still capable of detecting/receiving the position of any drone under Military USSP's control, even when the UAS is deviating from its intended flight plan.
- Detect e-conspicuous manned traffic prior it enters the U-space airspace.
- Provide real-time position of all other crewed and uncrewed aircraft.
  - Manned aircraft position data provided by the ATSP via sCISP.
  - Manned e-conspicuous aircraft position data provided by USSP.
  - Unmanned aircraft position data provided by USSP via the Network Identification Service as traffic information to the UAS operator/pilot.

The figure below shows an overview of Scenario 3 organisational structure and the communication/data links between the relevant stakeholders.

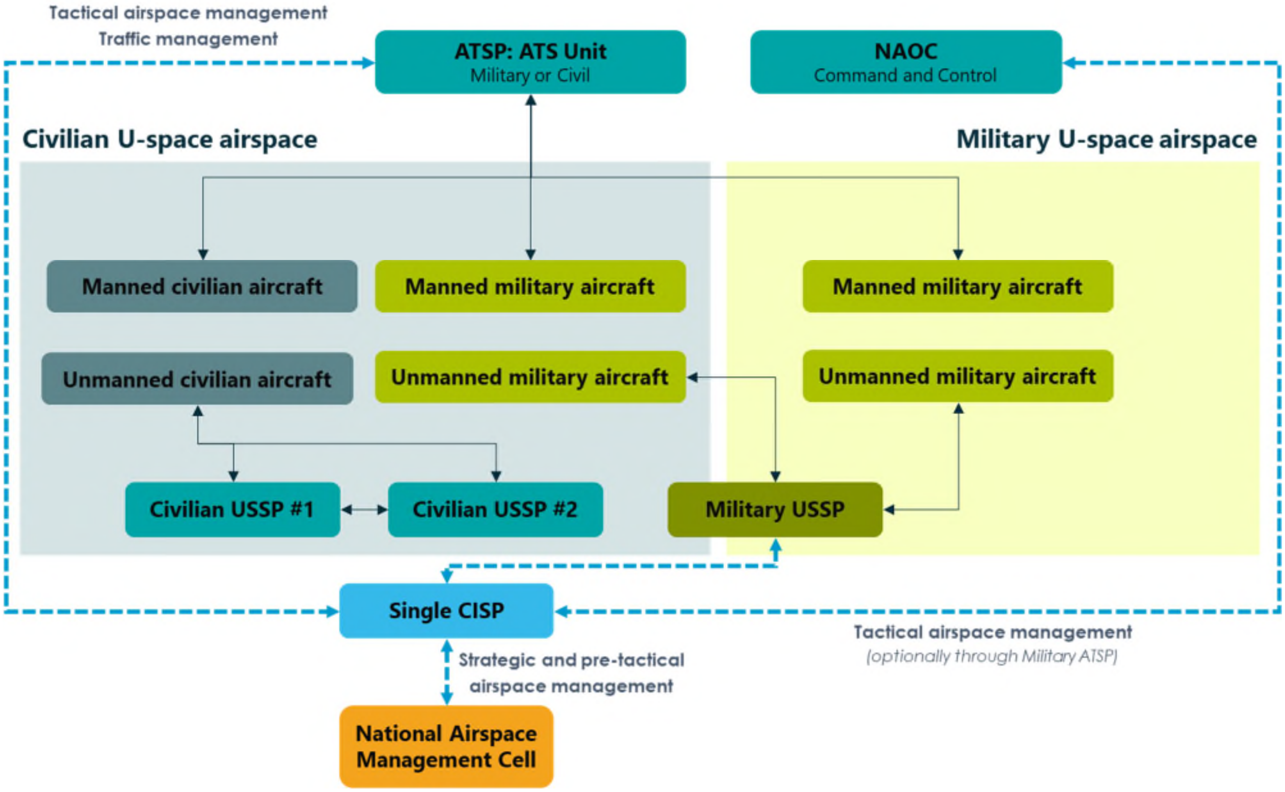
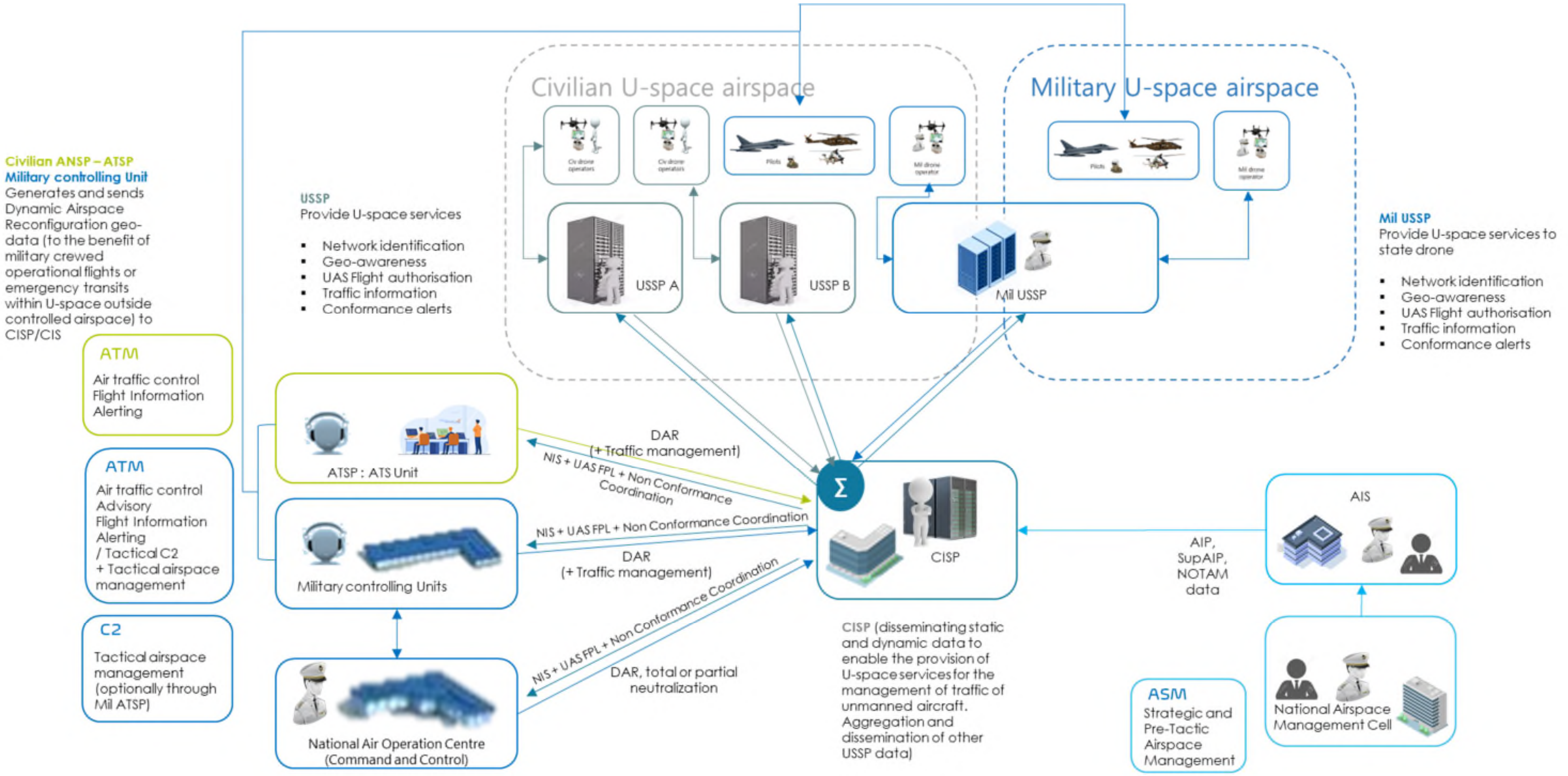


FIGURE 10: SCENARIO 3 ORGANISATIONAL OVERVIEW


Civilian U-space airspace
Military U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
Pilots
Mil drone operator
USSP A
USSP B
Mil USSP
ATM
Air traffic control
Flight Information
Alerting
ATSP : ATS Unit
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management
Military controlling Units
C2
Tactical airspace management (optionally through Mil ATSP)
National Air Operation Centre (Command and Control)
DAR
(+ Traffic management)
NIS + UAS FPL + Non Conformance Coordination
NIS + UAS FPL + Non Conformance Coordination
DAR
(+ Traffic management)
NIS + UAS FPL + Non Conformance Coordination
DAR, total or partial neutralization
Σ
CISP
AIS
AIP,
SupAIP,
NOTAM
data
ASM
Strategic and Pre-Tactic Airspace Management
National Airspace Management Cell

Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS

USSP
Provide U-space services

- Network identification
- Geo-awareness
- UAS Flight authorisation
- Traffic information
- Conformance alerts

Mil USSP
Provide U-space services to state drone

- Network identification
- Geo-awareness
- UAS Flight authorisation
- Traffic information
- Conformance alerts

CISP (disseminating static and dynamic data to enable the provision of U-space services for the management of traffic of unmanned aircraft. Aggregation and dissemination of other USSP data)

FIGURE 11: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 3) – CENTRALISED MODEL (SINGLE CISP)

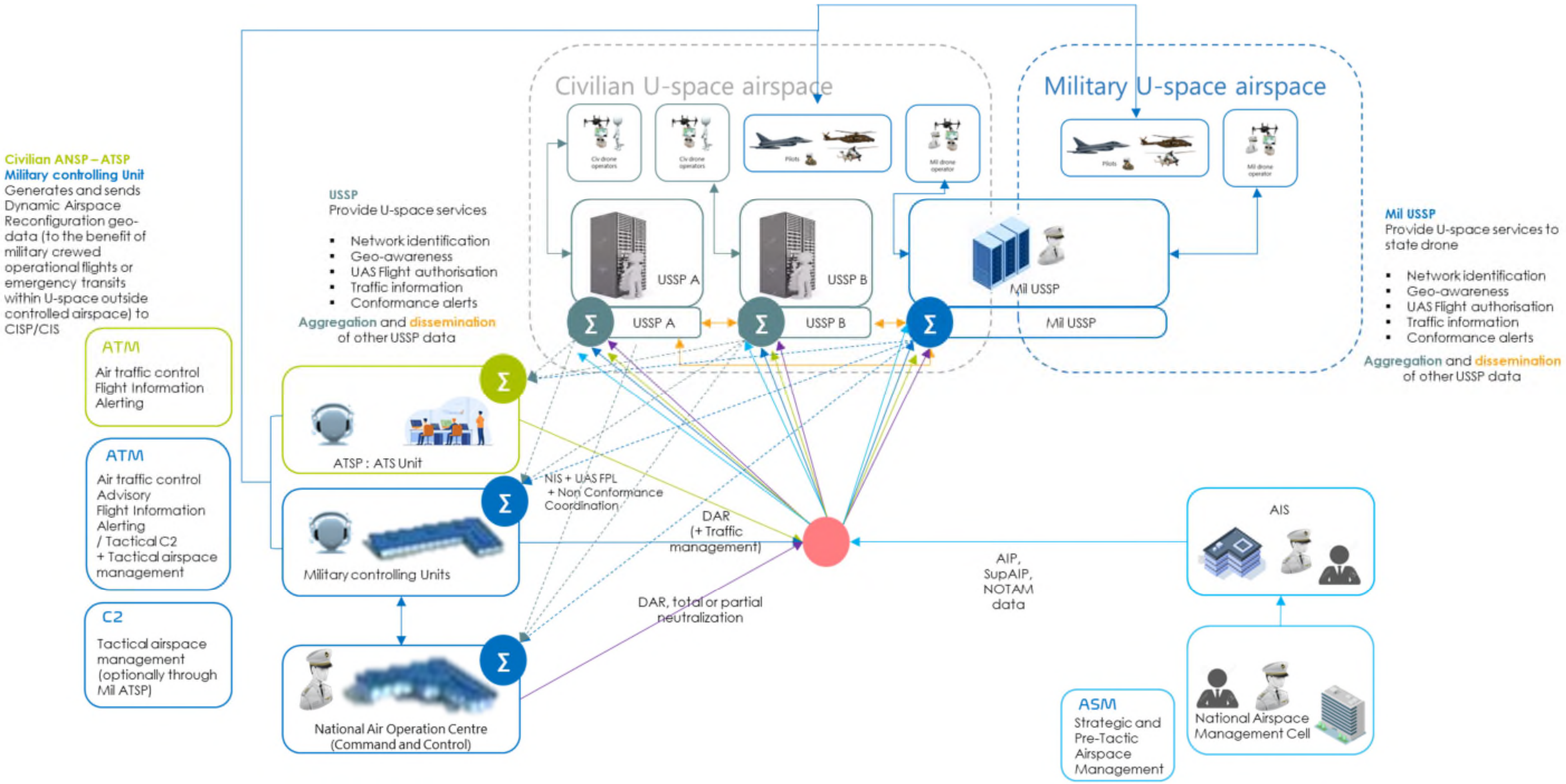

Civilian U-space airspace
Military U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
Pilots
Mil drone operator
Civilian ANSP – ATSP
Military controlling Unit
Generates and sends Dynamic Airspace Reconfiguration geo-data (to the benefit of military crewed operational flights or emergency transits within U-space outside controlled airspace) to CISP/CIS
USSP
Provide U-space services
▪ Network identification
▪ Geo-awareness
▪ UAS Flight authorisation
▪ Traffic information
▪ Conformance alerts
Aggregation and dissemination of other USSP data
USSP A
USSP B
Mil USSP
Σ USSP A
Σ USSP B
Σ Mil USSP
Mil USSP
Provide U-space services to state drone
▪ Network identification
▪ Geo-awareness
▪ UAS Flight authorisation
▪ Traffic information
▪ Conformance alerts
Aggregation and dissemination of other USSP data
ATM
Air traffic control
Flight Information
Alerting
ATM
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+ Tactical airspace management
C2
Tactical airspace management (optionally through Mil ATSP)
Σ
ATSP : ATS Unit
Σ
Military controlling Units
Σ
National Air Operation Centre (Command and Control)
NIS + UAS FPL + Non Conformance Coordination
DAR (+ Traffic management)
DAR, total or partial neutralization
AIP, SupAIP, NOTAM data
AIS
ASM
Strategic and Pre-Tactic Airspace Management
National Airspace Management Cell

FIGURE 12: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 3) – DISTRIBUTED MODEL (NO CISP)

4.1.5.1 - Impact of the scenario

The investments of the Military include developing and deploying a USS platform/system with the capabilities described under this scenario. The USS system supporting infrastructure (e.g. antennas, sensors, etc.) should be established to enable service provision. Furthermore, qualified personnel should be hired or trained to operate the system.

In return, as a USSP, the military would have a freedom of action and guaranteed sovereignty in supporting operations of state drones during public service, military missions or protection forces operations. In this scenario, the military would still have to establish communication/data links with the relevant stakeholders, as described in Scenarios 0, 1 and 2.

4.1.6 - Scenario 4: pan-European military USSP

The Scenario 4 envisages the existence of a single pan-European military USSP. The Member State's choice of organisational model (A, B, C mentioned explained within Scenario 1 in section 4.1.3 -) has no impact on the operational benefits that the services of the U-space ecosystem would bring to military. In this scenario, the military will:

- Retain the responsibilities of UAS geographical zone manager as described in Scenario 0.
- Retain benefits described as part of the Scenario 1 (consumer of U-space services).
- Share information about manned military aircraft within the U-space through national single CISPs, as part of Scenario 2 (provider of information to CISP).

An organisation of a pan-European military USSP could only be based on homogeneity of military USSP systems and delegation of responsibility and sovereignty. For cross-border operations, the USSP shall have two communication links with national single CISPs in order to share the data. A single European CISP entity would be able to tackle such challenges with a minimum duplication of data/communication links, but no such entity is planned to be created at this point in time.

4.1.6.1 - Impact of the scenario

The pan-European military USSP requires investments in the same areas as local USSP (e.g. USS system, sensors and supporting infrastructure), although the order of magnitude might be different.

Just like for Scenario 3, the benefits related to sovereignty and freedom of action are applicable to this scenario as well. On the top of these benefits, the financial investments will be lower than for Scenario 3, when compared to cumulative investments into individual military USSPs in the European region. Similarly to Scenarios 0 to 3, the military should still establish communication/data links with the relevant stakeholders.

The figure below shows an overview of Scenario 4 organisational structure and the communication/data links between the relevant stakeholders.

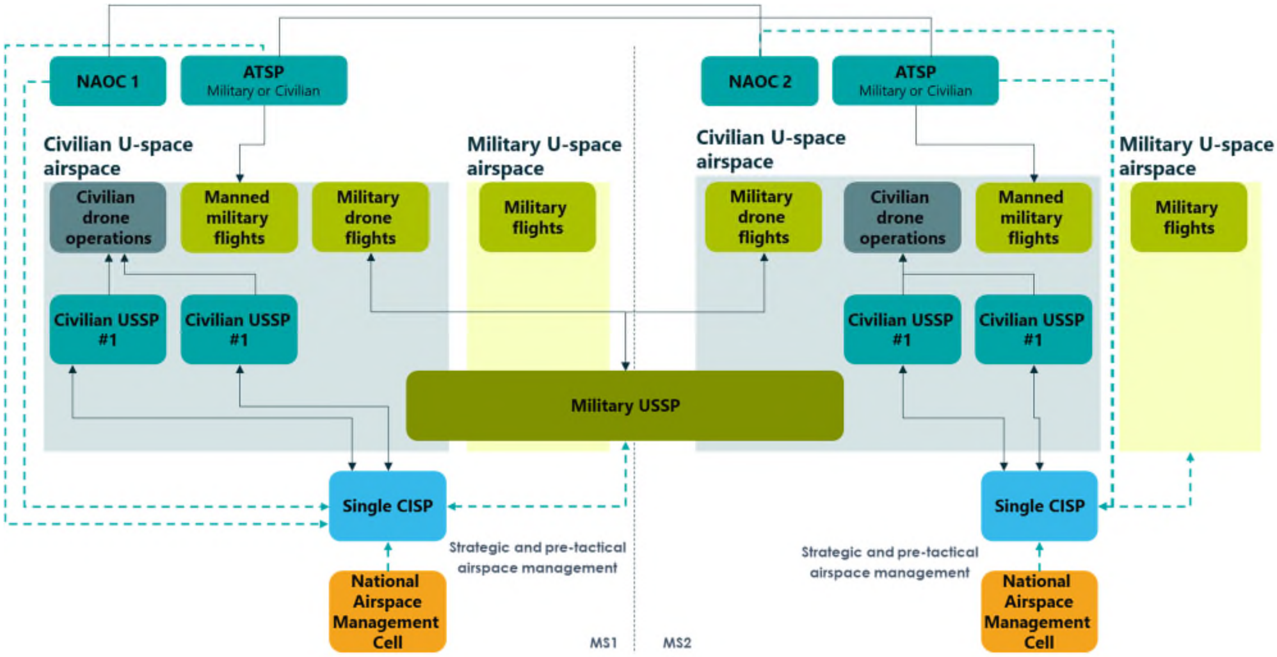

NAOC 1
ATSP
Military or Civilian
NAOC 2
ATSP
Military or Civilian
Civilian U-space airspace
Military U-space airspace
Civilian U-space airspace
Military U-space airspace
Civilian drone operations
Manned military flights
Military drone flights
Military flights
Military drone flights
Civilian drone operations
Manned military flights
Military flights
Civilian USSP #1
Civilian USSP #1
Civilian USSP #1
Civilian USSP #1
Military USSP
Single CISP
Single CISP
Strategic and pre-tactical airspace management
Strategic and pre-tactical airspace management
National Airspace Management Cell
National Airspace Management Cell
MS1
MS2

FIGURE 13: SCENARIO 4 ORGANISATIONAL OVERVIEW

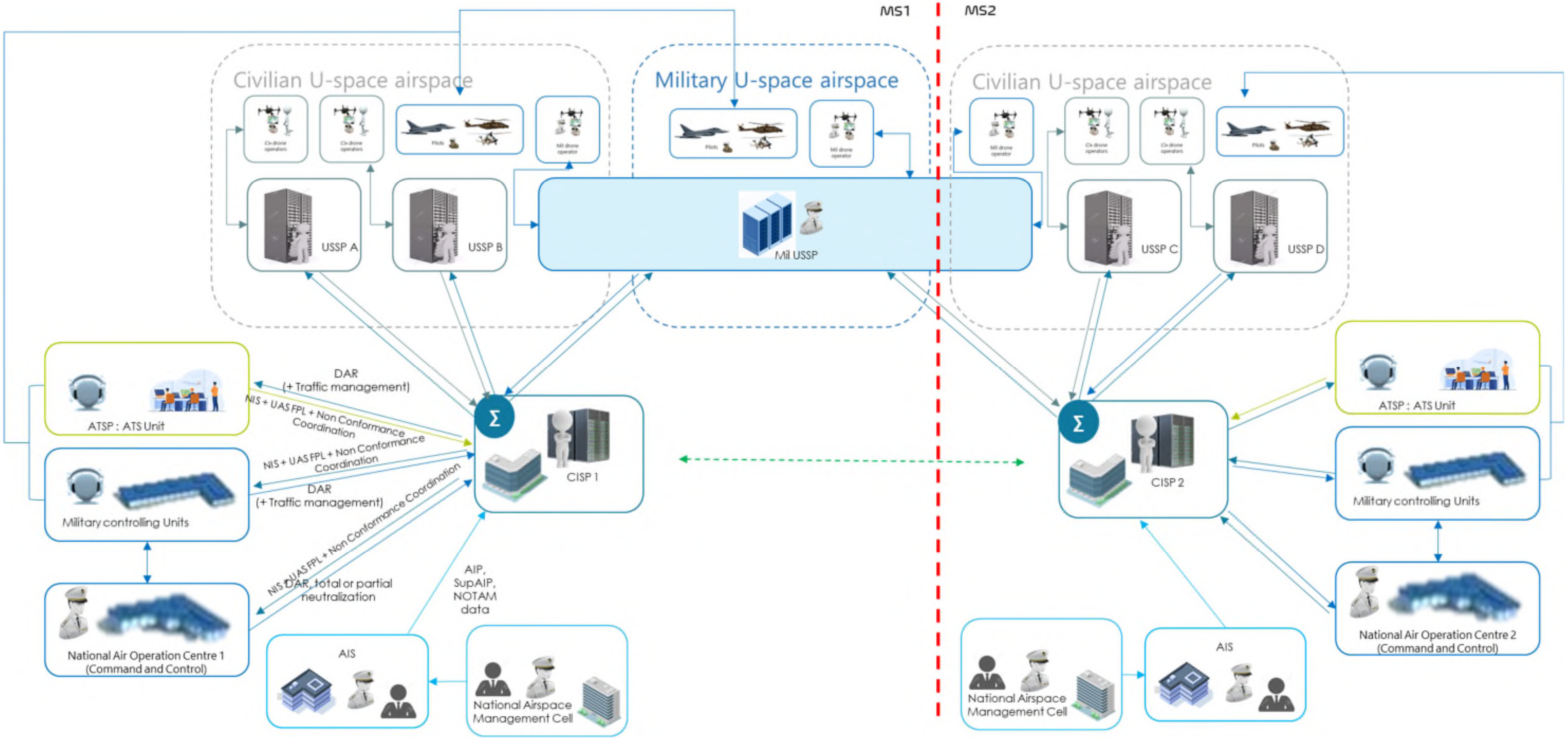


FIGURE 14: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 4) – CENTRALISED MODEL/CENTRALISED MODEL (SINGLE CISPS IN ALL MS)

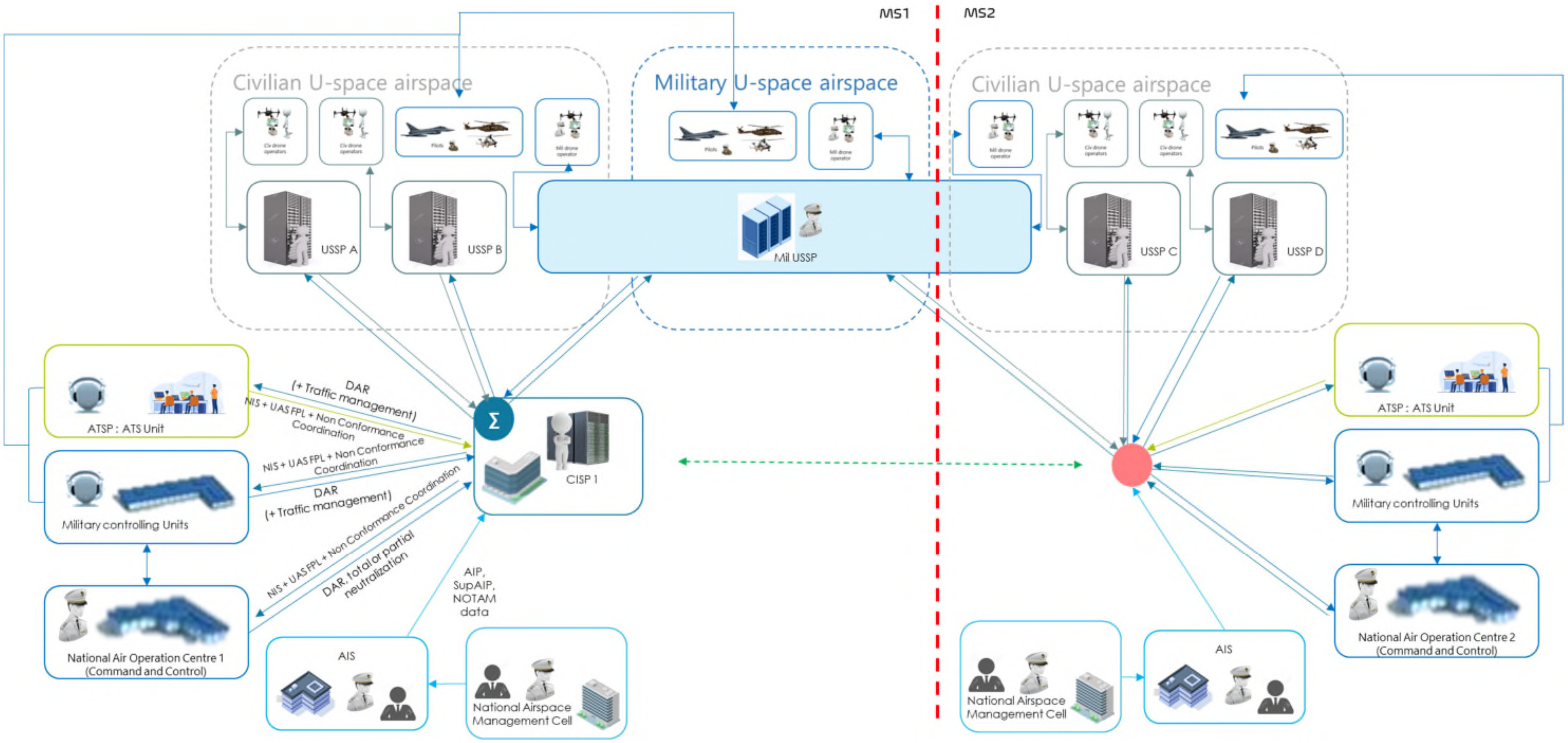

MS1
MS2
Civilian U-space airspace
Civ drone operators
Civ drone operators
Pilots
Mil drone operator
USSP A
USSP B
Military U-space airspace
Pilots
Mil drone operator
Mil USSP
Civilian U-space airspace
Mil drone operator
Civ drone operators
Civ drone operators
Pilots
USSP C
USSP D
ATSP : ATS Unit
DAR
(+ Traffic management)
NIS + UAS FPL + Non Conformance Coordination
Military controlling Units
NIS + UAS FPL + Non Conformance Coordination
DAR
(+ Traffic management)
NIS + UAS FPL + Non Conformance Coordination
DAR, total or partial neutralization
Σ
CISP 1
National Air Operation Centre 1 (Command and Control)
AIS
AIP, SupAIP, NOTAM data
National Airspace Management Cell
ATSP : ATS Unit
Military controlling Units
National Air Operation Centre 2 (Command and Control)
National Airspace Management Cell
AIS

FIGURE 15: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 4) – CENTRALISED MODEL/DISTRIBUTED MODEL (SINGLE CISP IN ONE MS)

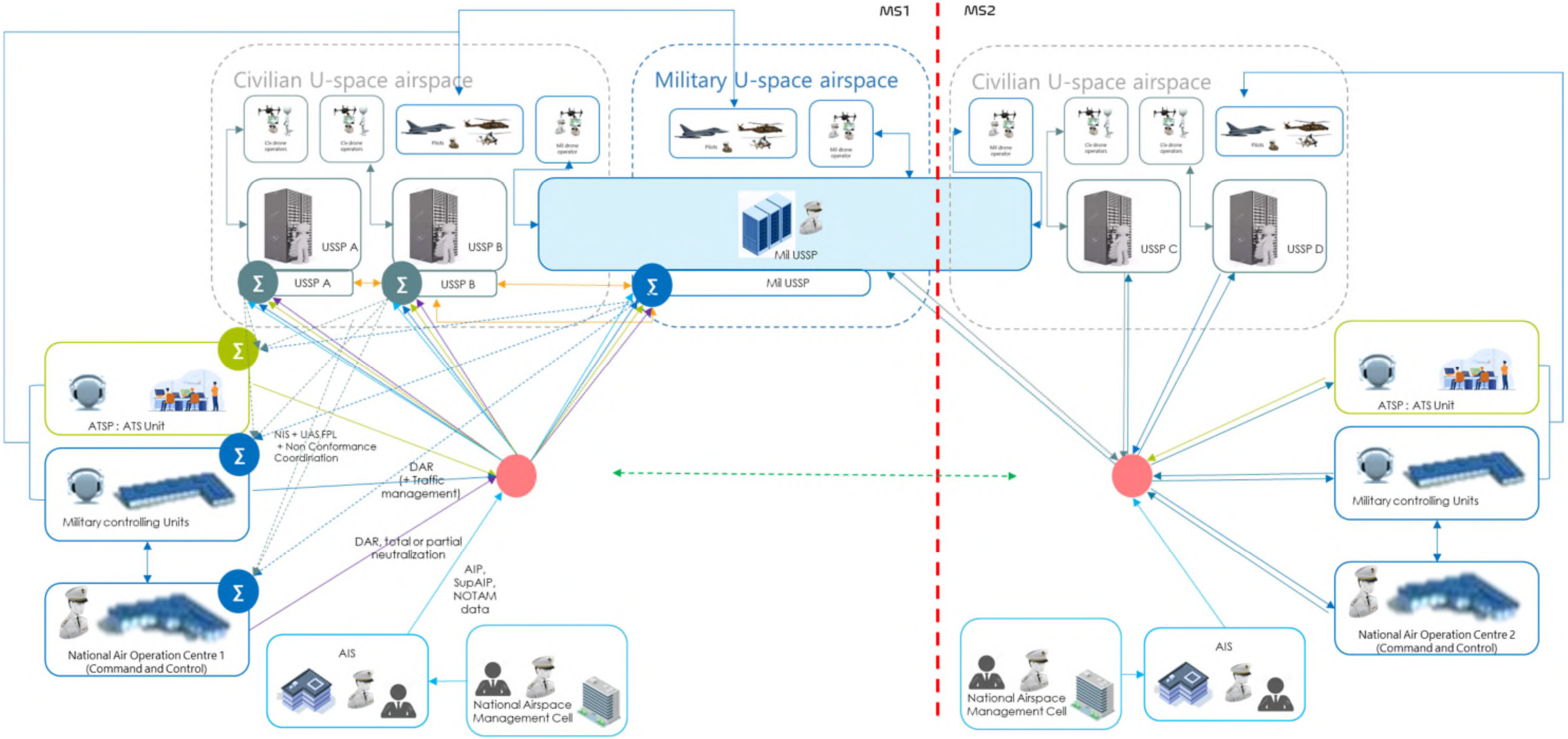


FIGURE 16: INFORMATION FLOWS FOR U-SPACE SERVICES (SCENARIO 4) – DISTRIBUTED MODEL/DISTRIBUTED MODEL (NO CISP IN EITHER MS)

4.2 - Comparative assessment of operational scenarios

4.2.1 - SWOT approach

SWOT analysis is a technique used to identify the strengths, weaknesses, opportunities and threats surrounding a business or an organisation. Analysing these four factors gives a broader picture of its situation and how it can evolve.

- **Strengths** refer to internal initiatives that perform well. Analysis of this factor may involve comparison to other initiatives or to an external competitive advantage.
- **Weaknesses** refer to less successful internal initiatives. It is customary to analyse strengths before weaknesses in order to establish a baseline for successes and failures. Identifying internal weaknesses is a starting point for improving organisations or projects.
- **Opportunities** are the result of current strengths and weaknesses, as well as any external initiatives that will place the organisation in a stronger competitive position. These may be weaknesses on which to improve or areas that were not identified as strengths or weaknesses in the previous steps.
- **Threats** refer to areas that can cause problems. They differ from weaknesses in that they are external and generally beyond the control of the organisation.

The comparative SWOT analysis will be performed across the six defined criteria in order to properly and completely assess the viability of the proposed scenarios of the military involvement in U-Space. This analysis is designed to provide decision-making entities like the MoD with a robust framework for evaluating each scenario's potential strengths, weaknesses, opportunities, and threats and assessing what would be the best option for the military in U-space at a national level.

Through this comparative analysis, the decision-makers can gain valuable insights into how each scenario aligns with the unique demands and challenges of U-Space military operations. Furthermore, this analysis highlights the inherent trade-offs associated with each scenario.

Additionally, the comparative analysis enables a comprehensive view of the strategic landscape, considering both immediate operational requirements and long-term sustainability. This holistic approach is essential in the dynamic and evolving domain of U-Space, where technological advancements and geopolitical shifts continuously reshape the operating environment.

Moreover, evaluating multiple scenarios concurrently facilitates the identification of synergies and integration opportunities. Elements from different scenarios may complement each other, offering a more comprehensive solution to address a broader range of military objectives.

In conclusion, conducting a comparative SWOT analysis of the five proposed scenarios using a well-defined criteria framework provides the relevant military stakeholders with a structured approach to evaluate their suitability for the potential military roles in U-Space.

4.2.2 - Definition of assessment criteria

Developing comprehensive assessment criteria is crucial for accurately evaluating the impact of various scenarios for the military within U-space. Clear and structured criteria enable the military stakeholders to effectively assess implications, make informed decisions, and mitigate potential risks.

Each criterion evaluates different aspects, from governance and regulatory compliance to operational efficiency and financial sustainability. Systematic assessment provides key features of each scenario, allowing for well-informed decisions aligned with military objectives. Ultimately, robust assessment criteria optimize U-space implementation while safeguarding military interests and operational effectiveness.

Six criteria have been identified to address critical aspects essential for military engagement in U-space operations, taking into account the distinct requirements of each scenario:

- **Governance criterion (G)**

Assessing the governance of U-space involves scrutinising the structure overseeing its management and operations. The clarity and effectiveness of this governance structure are essential for efficient decision-making processes and transparent accountability.

Evaluation extends to the establishment of coordination frameworks with relevant national and international authorities, ensuring seamless integration and alignment with broader regulatory frameworks. Effective governance fosters collaboration and facilitates the implementation of U-space initiatives in a manner that promotes safety, interoperability, and efficiency.

- **Regulatory criterion (R)**

Regulatory criterion encompasses the adherence to regulatory frameworks governing both military operations and U-space activities. Alignment with U-space regulations ensures compliance with safety standards and interoperability requirements. Compatibility with military standards, such as NATO STANAGs[8], is crucial for facilitating coordination and integration with military operations.

Additionally, compliance with wider ATM and UTM industry standards ensures harmonisation within the broader airspace management ecosystem, fostering interoperability and cooperation among stakeholders.

- **Operational criterion (O)**

Operational criterion is focused on the practical aspects of providing air traffic services to both manned and unmanned aircraft within U-space. Evaluation includes the ability to handle diverse air traffic types efficiently, ensuring smooth operations and minimising disruptions.

Coordination mechanisms with adjacent airspace are critical for managing airspace boundaries and ensuring safe operations. Assessing operational performance involves examining metrics such as reliability, responsiveness, and safety to gauge the effectiveness of U-space operations.

- **Technical criterion (T)**

The technical criterion encompasses the technological facets essential for the successful implementation of U-space, considering integration with both military and civil systems. Compatibility with existing military systems facilitates seamless integration and interoperability within established military airspace management infrastructure while ensuring harmonisation with civil systems. By incorporating technological advancements tailored to meet military requirements, operational efficiency and safety are enhanced, encouraging the adoption of innovative solutions for airspace management within U-space.

Effective data exchange capabilities enable real-time information sharing, supporting situational awareness and informed decision-making, while also facilitating collaboration with civil counterparts.

- **Financial criterion (F)**

Financial criterion assesses the economic viability and sustainability of U-space scenarios with considerations for MoD budget constraints. Evaluating cost-efficiency involves considering both initial investment and ongoing operational costs related to the military involvement in U-space operations, ensuring that resources are allocated effectively. Identifying potential revenue streams and evaluating their long-term sustainability is crucial for ensuring financial stability of military U-space initiatives.

Accurate financial forecasts enable realistic planning and budgeting, ensuring that U-space initiatives align with military priorities and are financially feasible within ministry of defence budgetary constraints.

Moreover, identifying suitable funding mechanisms is essential for securing the necessary resources to support the implementation and sustainability of U-space operations when military has an active role.

- **Manpower criterion (M)**

The Manpower criterion assesses the readiness of current military personnel for U-space tasks, identifying training needs and recruitment strategies to meet operational demands. It evaluates skill levels, addresses gaps through tailored training, and optimises workforce utilisation for efficiency and safety within military U-space operations.

[8] *NATO Standardization Agreements for procedures and systems and equipment components; developed and promulgated by the NATO Standardization Agency in conjunction with the Conference of National Armaments Directors and other authorities concerned. (Source: https://www.nato.int/cps/fr/natohq/stanag.htm)*

By ensuring personnel is adequately trained and deployed, the criterion aims to uphold operational effectiveness and support military objectives in the dynamic U-space environment.

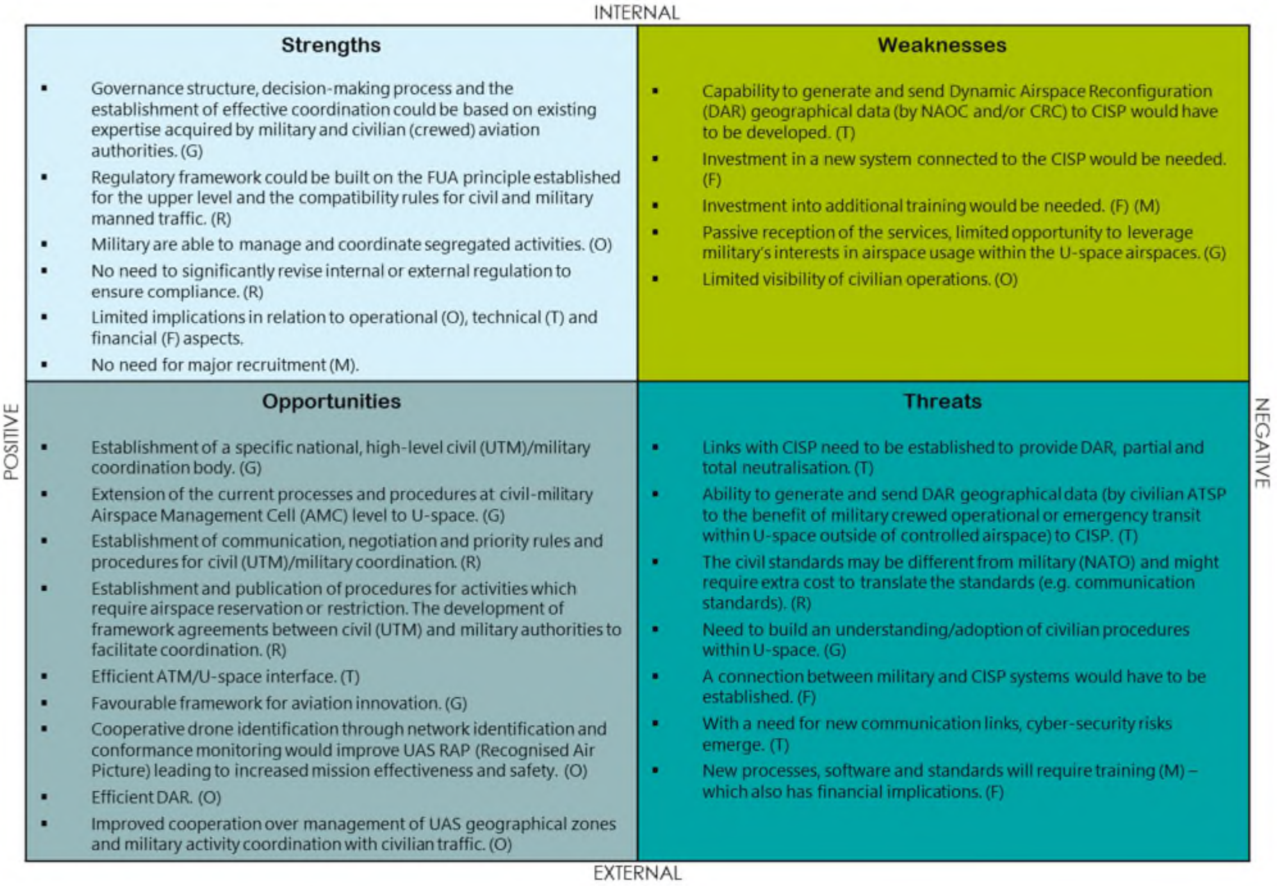
4.2.3 - SWOT analysis

The outcome of the SWOT analysis for each scenario considered in SC4 is provided as a set of tables (one per scenario), which detail the assessment of the scenario according to the criteria defined in the previous section and organised into strengths, weaknesses, opportunities and threats.

These tables can be read in different ways, which help develop a comprehensive understanding of each scenario when brought together:

- Each box in the table lists the argument supporting the assessment of each criterion as strengths, weaknesses, opportunities and threats. There can be different aspects (e.g. a strength and a weakness, or several opportunities) associated to a same criterion;
- The top row (strengths and weaknesses) represents internal factors, i.e. those that the military can influence directly, while the bottom row (opportunities and threats) are external factors, i.e. outside the direct control of the military). Therefore, a table featuring a top row with more arguments than the bottom row means that the military will generally have better control on the outcome of the scenario.
- The left column (strengths and opportunities) corresponds to positives and the right column to negatives. A table with more arguments in the left column than in the right one generally describes a better outcome.

4.2.3.1 - Scenario 0: UAS geographical zone manager



INTERNAL

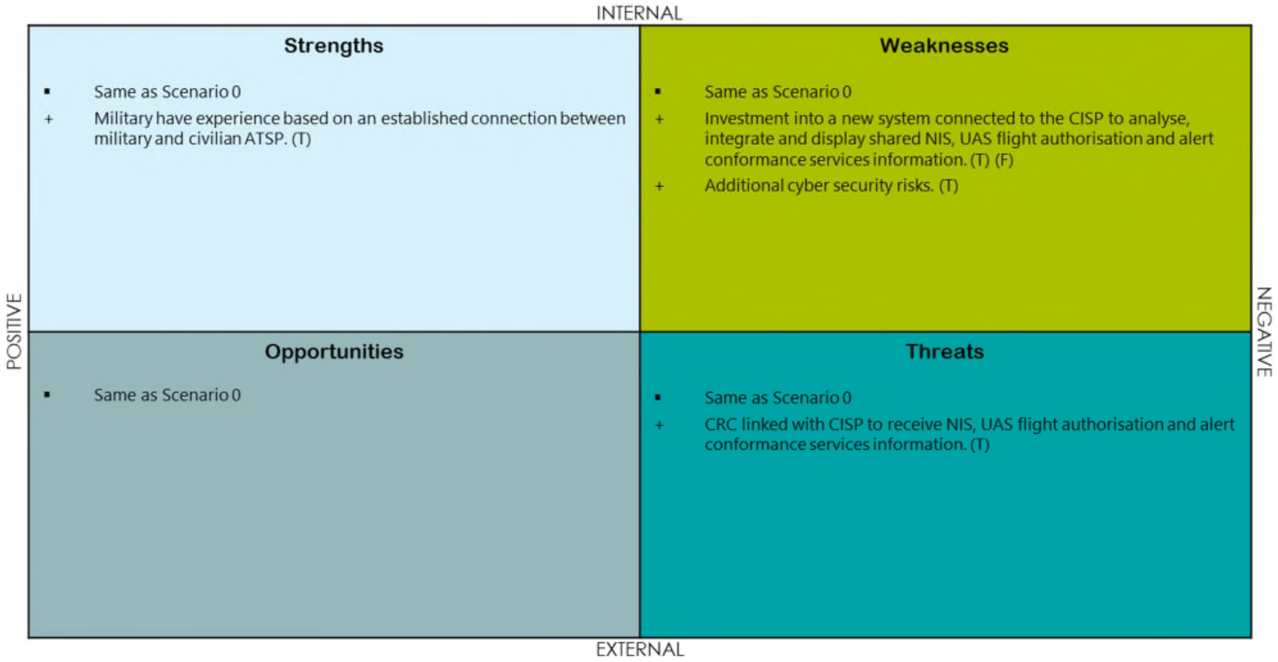
Strengths	Weaknesses
▪ Governance structure, decision-making process and the establishment of effective coordination could be based on existing expertise acquired by military and civilian (crewed) aviation authorities. (G) ▪ Regulatory framework could be built on the FUA principle established for the upper level and the compatibility rules for civil and military manned traffic. (R) ▪ Military are able to manage and coordinate segregated activities. (O) ▪ No need to significantly revise internal or external regulation to ensure compliance. (R) ▪ Limited implications in relation to operational (O), technical (T) and financial (F) aspects. ▪ No need for major recruitment (M).	▪ Capability to generate and send Dynamic Airspace Reconfiguration (DAR) geographical data (by NAOC and/or CRC) to CISP would have to be developed. (T) ▪ Investment in a new system connected to the CISP would be needed. (F) ▪ Investment into additional training would be needed. (F) (M) ▪ Passive reception of the services, limited opportunity to leverage military's interests in airspace usage within the U-space airspaces. (G) ▪ Limited visibility of civilian operations. (O)
Opportunities	**Threats**
▪ Establishment of a specific national, high-level civil (UTM)/military coordination body. (G) ▪ Extension of the current processes and procedures at civil-military Airspace Management Cell (AMC) level to U-space. (G) ▪ Establishment of communication, negotiation and priority rules and procedures for civil (UTM)/military coordination. (R) ▪ Establishment and publication of procedures for activities which require airspace reservation or restriction. The development of framework agreements between civil (UTM) and military authorities to facilitate coordination. (R) ▪ Efficient ATM/U-space interface. (T) ▪ Favourable framework for aviation innovation. (G) ▪ Cooperative drone identification through network identification and conformance monitoring would improve UAS RAP (Recognised Air Picture) leading to increased mission effectiveness and safety. (O) ▪ Efficient DAR. (O) ▪ Improved cooperation over management of UAS geographical zones and military activity coordination with civilian traffic. (O)	▪ Links with CISP need to be established to provide DAR, partial and total neutralisation. (T) ▪ Ability to generate and send DAR geographical data (by civilian ATSP to the benefit of military crewed operational or emergency transit within U-space outside of controlled airspace) to CISP. (T) ▪ The civil standards may be different from military (NATO) and might require extra cost to translate the standards (e.g. communication standards). (R) ▪ Need to build an understanding/adoption of civilian procedures within U-space. (G) ▪ A connection between military and CISP systems would have to be established. (F) ▪ With a need for new communication links, cyber-security risks emerge. (T) ▪ New processes, software and standards will require training (M) – which also has financial implications. (F)

POSITIVE

NEGATIVE

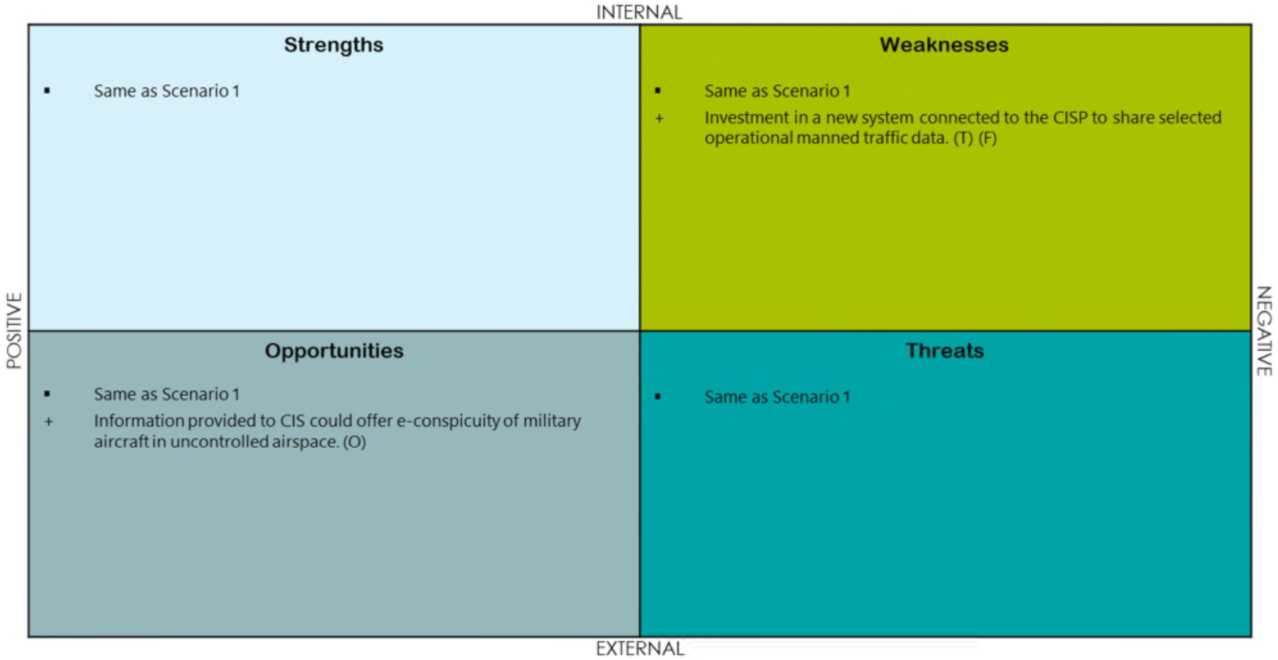
EXTERNAL

4.2.3.2 - Scenario 1: consumer of U-space services



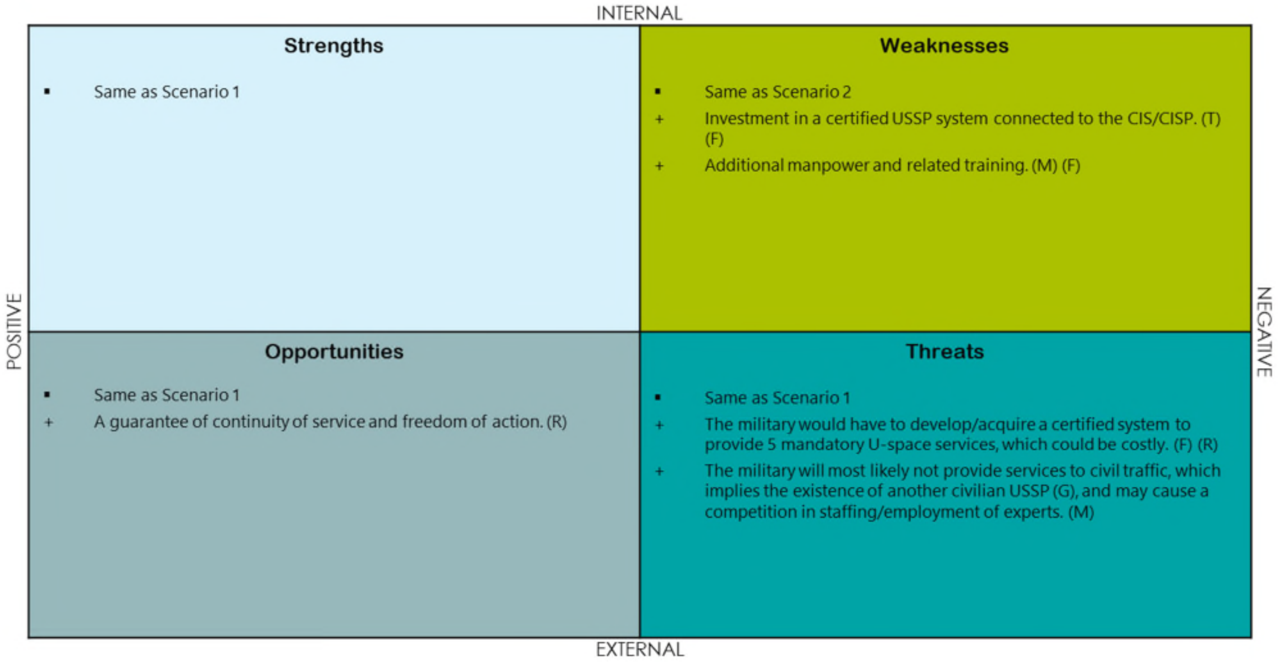
	POSITIVE	NEGATIVE
INTERNAL	**Strengths** ▪ Same as Scenario 0 + Military have experience based on an established connection between military and civilian ATSP. (T)	**Weaknesses** ▪ Same as Scenario 0 + Investment into a new system connected to the CISP to analyse, integrate and display shared NIS, UAS flight authorisation and alert conformance services information. (T) (F) + Additional cyber security risks. (T)
EXTERNAL	**Opportunities** ▪ Same as Scenario 0	**Threats** ▪ Same as Scenario 0 + CRC linked with CISP to receive NIS, UAS flight authorisation and alert conformance services information. (T)

4.2.3.3 - Scenario 2: consumer and provider of information to CIS



	POSITIVE	NEGATIVE
INTERNAL	**Strengths** ▪ Same as Scenario 1	**Weaknesses** ▪ Same as Scenario 1 + Investment in a new system connected to the CISP to share selected operational manned traffic data. (T) (F)
EXTERNAL	**Opportunities** ▪ Same as Scenario 1 + Information provided to CIS could offer e-conspicuity of military aircraft in uncontrolled airspace. (O)	**Threats** ▪ Same as Scenario 1

4.2.3.4 - Scenario 3: national military USSP



INTERNAL

POSITIVE

NEGATIVE

EXTERNAL

Strengths

▪ Same as Scenario 1

Weaknesses

▪ Same as Scenario 2

+ Investment in a certified USSP system connected to the CIS/CISP. (T) (F)

+ Additional manpower and related training. (M) (F)

Opportunities

▪ Same as Scenario 1

+ A guarantee of continuity of service and freedom of action. (R)

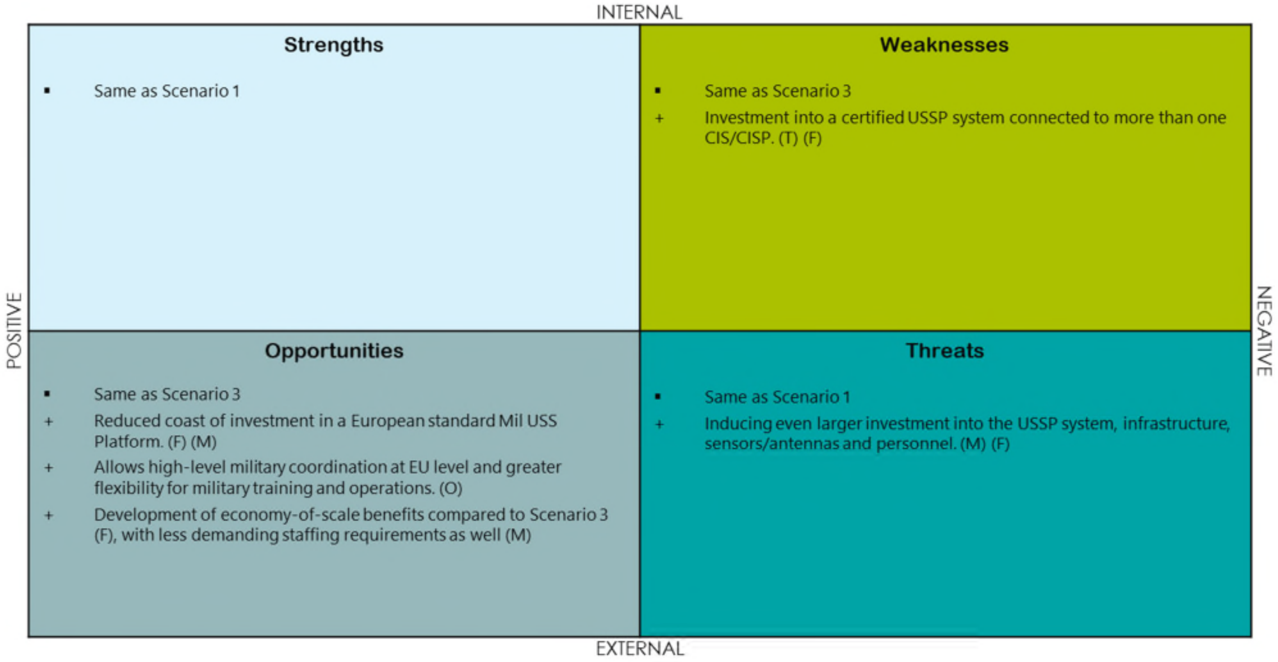
Threats

▪ Same as Scenario 1

+ The military would have to develop/acquire a certified system to provide 5 mandatory U-space services, which could be costly. (F) (R)

+ The military will most likely not provide services to civil traffic, which implies the existence of another civilian USSP (G), and may cause a competition in staffing/employment of experts. (M)

4.2.3.5 - Scenario 4: pan-European military USSP



INTERNAL

POSITIVE

NEGATIVE

EXTERNAL

Strengths

▪ Same as Scenario 1

Weaknesses

▪ Same as Scenario 3

+ Investment into a certified USSP system connected to more than one CIS/CISP. (T) (F)

Opportunities

▪ Same as Scenario 3

+ Reduced coast of investment in a European standard Mil USS Platform. (F) (M)

+ Allows high-level military coordination at EU level and greater flexibility for military training and operations. (O)

+ Development of economy-of-scale benefits compared to Scenario 3 (F), with less demanding staffing requirements as well (M)

Threats

▪ Same as Scenario 1

+ Inducing even larger investment into the USSP system, infrastructure, sensors/antennas and personnel. (M) (F)

4.3 - Conclusions/preferred operational scenario(s)

4.3.1 - SWOT analysis summary

4.3.1.1 - Summary of Strengths

Scenario 0: there are three key advantages linked to Scenario 0. They are linked to a general overview of the activities, strengthened decision-making position and coordination with civilian traffic management (segregated activities). Scenario 0 could be built upon existing regulatory principles and existing standards, thus avoiding complicated restructuring and investment into systems and personnel (training).

Scenarios 1 – 4: On top of the Scenario 0 benefits, the Military could benefit from their previous experience in civilian and military ATSP cooperation.

4.3.1.2 - Summary of Weaknesses

The challenges of the Military across all scenarios are mostly financial and technical as they require implementation of new systems or platforms and associated training. Such a transition would require a phased approach and significant investments.

Scenario 0: a system/capability to produce and share geographical data with the CISP/CIS for DAR purposes would have to be developed. Furthermore, appropriate training of staff involved in U-space processes would be required.

Under **Scenario 1**, the new system would require slightly greater investment as it should also be able to process data received through U-space service (network identification, UAS flight authorisations and conformance monitoring). With these additional interfaces, the Military would also have to consider the associated cyber security risks. In **Scenario 2**, the system would also be connected to the CISP/CIS to share selected operational manned traffic data. On top of these limitations, further investments into a certified USSP system and manpower (recruitment/training) would be required under **Scenario 3**. The USSP system for **Scenario 4** is expected to be more sophisticated and technically complex, thus more expensive.

4.3.1.3 - Summary of Opportunities

Scenario 0 and 1: the establishment of a specific national high-level civil/military coordination body is considered as an opportunity for wider collaboration at the U-space level. The processes and procedures at the civil-military Airspace Management Cell (AMC) level can be expanded to cover the U-space airspaces. The communication, negotiation and priority rules and procedures for civil UTM/military coordination would need to be established.

Under **Scenario 2**, providing military-specific information within the U-space through the CISP/CIS could include surveillance tracks of military aircraft that operate or transit in the U-space airspace, thereby compensating for a possible lack of e-conspicuity capabilities in uncontrolled airspace and increasing the level of safety. In **Scenario 3**, the military as an USSP would have a freedom of action and guaranteed sovereignty in supporting operations of state drones during public service, military missions or operations of protection forces. The military would still need to establish communication and data links with the relevant stakeholders. In **Scenario 4**, a pan-European military USSP would require investments in areas similar to those of national USSPs. However, these investments are considerably lower compared to the total investments into individual military USSPs across Europe as in Scenario 3. A pan-European military USSP would require lower number of highly qualified staff which had been in high demand in aviation industry in the recent years.[9]

[9] IFATCA EVP Europe on the European staff shortage, 2023

4.3.1.4 - Threats to mitigate

In **Scenario 0**, the coordination between NAOC/ATS and the CISP/CIS would enable the civilian ATSP to generate and share the geographical data resulting from DAR. Connectivity between military and the CISP/CIS would have to be established but it might be pose number of challenges as civil and military standards may differ, thus requiring additional costs to translate these standards. With an increasing number of connectivity links, cyber-security risks and training requirements shall be considered.

Scenario 1 and 2: The deployment and maintenance of military systems, including the integration of CISP data, could lead to emerging cyber security risks. Appropriate tools and processes would have to be established to manage the risks. Moreover, utilising the UAS flight authorisation service may result in additional costs for deploying and maintaining military systems. Furthermore, Air Surveillance Operators and Tactical Controllers would need to undertake additional training to understand how to process and utilise the information provided by the Network Information Service and the Conformance Monitoring Service.

Under **Scenario 3 and 4**, the military would have to invest into the development and deployment of a USSP system. To facilitate service provision, the necessary infrastructure for this USSP system would have to be established. Additionally, qualified personnel would have to be hired or trained to operate the system.

4.3.2 - Strategic recommendations

The SWOT analysis performed on the various operational scenarios considered in SC4 do not allow identifying one scenario with clear benefits over the others. Rather, the different scenarios correspond to increased level of integration of the military into the U-space operational processes and technical systems, which provide increasing benefits in term of mission effectiveness and safety, but at the cost of increased financial investments and cyber security risks.

Although **Scenario 4** would provide significant economies of scale, it is probably too politically complex to be implemented in the short term. For a near future objective, **Scenarios 0** to **3** are thus more realistic options, and also leave each Member State to decide on their ambition regarding the involvement of their military in U-space. The most important step toward this objective would be for the military to acquire the connectivity with the CISP/CIS; once this is achieved, the gaps between **Scenarios 1**, **2** and **3** are limited. Consequently, aiming from the start for a higher level of integration (i.e. **Scenario 2** or **Scenario 3**) would be more efficient compared to a staged approach and would deliver important benefits more rapidly.

Lastly, it is interesting to note that the different scenarios assessed in SC4 are not mutually exclusive, but rather represent the incremental steps that allow reaching a high level of military integration with U-space. Therefore, a Member State looking to implement **Scenario 3** could build a programme to that effect, which first phases would correspond to **Scenarios 1** and **2**.

5 - SUPPORTING ORGANISATION FOR OPERATIONAL SCENARIO(S)

5.1 - Description of a typical military organisation

Any new military function related to U-space would have to fit within existing military organisations in order to minimise the complexity of the resulting organisation, to ensure operational effectiveness and limit disruption to the functions that are already implemented.

As already described in SC3 and in section 4 - of the present report, interacting or integrating with U-space potentially affects three main processes for the military:

- Airspace management;
- (manned) air traffic management and control;
- Air surveillance, in case the military chose to rely on U-space services to inform the RAP.

Therefore, the new military processes associated with U-space would have to fit as best as possible within the existing functions in charge of the above three processes. The existing functions are depicted in the following generic military organisation.

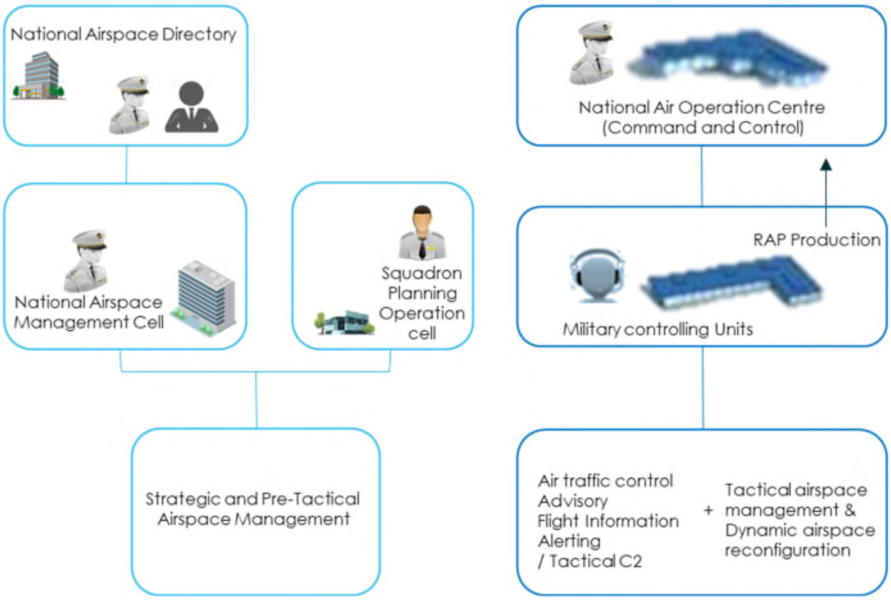

National Airspace Directory
National Air Operation Centre (Command and Control)
National Airspace Management Cell
Squadron Planning Operation cell
RAP Production
Military controlling Units
Strategic and Pre-Tactical Airspace Management
Air traffic control
Advisory
Flight Information
Alerting
/ Tactical C2
+
Tactical airspace management & Dynamic airspace reconfiguration

FIGURE 17: GENERIC MILITARY AVIATION FUNCTIONS AND ORGANISATION

SC3 has developed Use Cases that describe how these functions could interact with U-space to plan and manage military operations in U-space airspace in the pre-tactical and tactical phases without interfacing military system with the CISP/CIS. SC4 complements this initial work by investigating the impacts and possible benefits of developing this interface.

<u>Note:</u> the Navy and the Army are not considered in this report, while they also operate aircraft, helicopters and drones. In case they would also have to interact with U-space, SC4 assumes this would take place through coordination with the Air Force first, which would then act as intermediary an with U-space. SC4 thus does not anticipate that the Navy or the Army would require direct interaction with U-space.

5.2 - Benchmark of civilian ANSP organisations for U-space

Three civilian ANSPs[10] in the process of being certified as CISPs, and in some instances as USSPs, were consulted in the scope of SC4 to understand how these organisations are preparing for their new roles. Considering the organisational similarities between military and civilian ANSPs, the military could benefit from the experience of their civilian counterparts in case they would endorse new roles and responsibilities in the context of U-space.

The new organisations set up by these ANSPs are guided by two main drivers:

- The U-space regulatory framework, which defines in broad terms the responsibilities of CISPs and USSPs;
- A national initiative for the implementation of U-space designating a leading stakeholder, setting objectives for this implementation project, identifying the involved stakeholders and defining their respective roles.

In Spain, for example, the national implementation project is documented in a dedicated action plan ([11]), which notably defines the role of the Ministry of Defence in this project and the new responsibilities allocated to ENAIRE as single CISP for Spain, but also as USSP for drone operations conducted by actors from the public sector. Even though this type of local specificities impacts the detailed responsibilities of civilian ANSPs, and potentially their organisation, many commonalities have been found among the entities consulted for SC4.

All EU Member States currently implementing U-space have adopted the centralised U-space model (cf. Figure 2) and the civilian ANSP is or will be designated as the CISP for all U-space airspace in the country. Outside of the EU, Switzerland has rather opted for the distributed U-space model and skyguide, the civilian ANSP, is only involved in U-space as a provider of information to the CIS, with no impact on its organisational structure.

Civilian ANSPs designated as single CISPs are under a regulatory requirement to separate their CISP function from the ANSP function for financing reasons, as the European Commission wants to prevent air traffic charges from funding U-space implementation costs. This requirement does not apply to military organisations. Consequently, all the ANSPs consulted are currently implementing the CISP function as a new, distinct department within their existing structure. As a result, a same legal entity will now be hosting 2 (or 3 in the case of Spain) service providers, corresponding to model B (or model C in the case of Spain) in Figure 3. However, the different service providers share the same support functions (e.g. accounting, HR department, etc.).

5.3 - Definition of possible business models

In the private business sector, a business model can be represented in a simple graph called a business model canvas that helps understanding how a given business or set of services delivers and create value for both the company providing these services, the other companies involved along the value chain and ultimately the customer. In addition, this canvas allows identifying customer segments, delivery channels, key-partners, among other things.

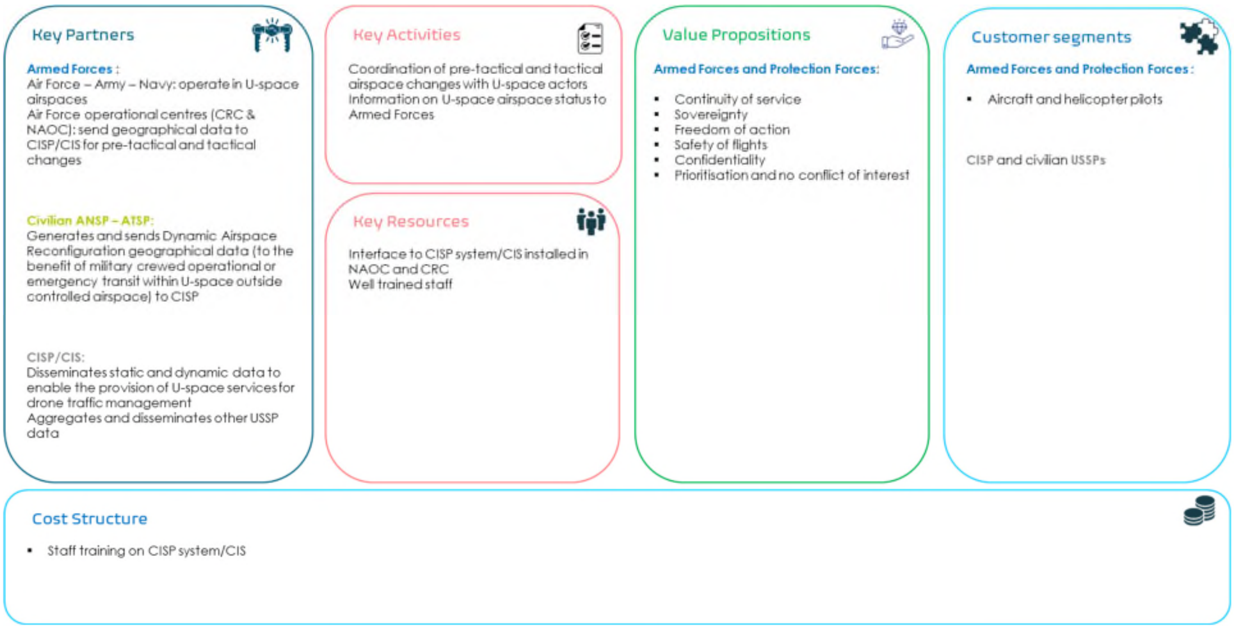
In the context of this study, the main purpose of the services under consideration, from the perspective of the military, is not to generate revenues but to improve the safety and the mission effectiveness of military operations. Even though the value generated by these services is not financial, a business model canvas is still useful to help understand how this value is generated and for who. Consequently, not all the objects found usually in a business model canvas are relevant and the diagrams presented in this section do not feature those focusing directly on the revenue side of a usual business model. The objects used in this simplified canvas are thus:

- **Key Partners**: who are the key partners and suppliers required to deliver the services? Which key resources are needed from them?
- **Key Activities**: what key activities do the value propositions require?
- **Key Resources**: what key resources do the value propositions require?

[10] skeyes for Belgium, ENAIRE for Spain and LFV for Sweden.

- **Value Propositions**: what value is delivered to the customer? Which services are provided to the customer segments? Which customer needs are these services satisfying?
- **Customer Segments**: for whom is value created? Which are the most important customers?
- **Cost Structure**: what are the most important costs inherent to the business model? Which key activities and resources are the most expensive?

Under **Scenario 0**, military operators in NAOCs and CRCs have a direct interface to the CISP system/CIS (not integrated with the military systems) allowing them to receive information on the status of U-space airspace and to request U-space airspace changes, whether in controlled or uncontrolled airspace. Thanks to this information, aircraft and helicopter can safely operate in U-space airspaces, even for unplanned missions. The corresponding business model is described by the following simplified canvas.



Key Partners

Armed Forces :
Air Force – Army – Navy: operate in U-space airspaces
Air Force operational centres (CRC & NAOC): send geographical data to CISP/CIS for pre-tactical and tactical changes

Civilian ANSP – ATSP:
Generates and sends Dynamic Airspace Reconfiguration geographical data (to the benefit of military crewed operational or emergency transit within U-space outside controlled airspace) to CISP

CISP/CIS:
Disseminates static and dynamic data to enable the provision of U-space services for drone traffic management
Aggregates and disseminates other USSP data

Key Activities

Coordination of pre-tactical and tactical airspace changes with U-space actors
Information on U-space airspace status to Armed Forces

Key Resources

Interface to CISP system/CIS installed in NAOC and CRC
Well trained staff

Value Propositions

Armed Forces and Protection Forces:

- Continuity of service
- Sovereignty
- Freedom of action
- Safety of flights
- Confidentiality
- Prioritisation and no conflict of interest

Customer segments

Armed Forces and Protection Forces :

- Aircraft and helicopter pilots

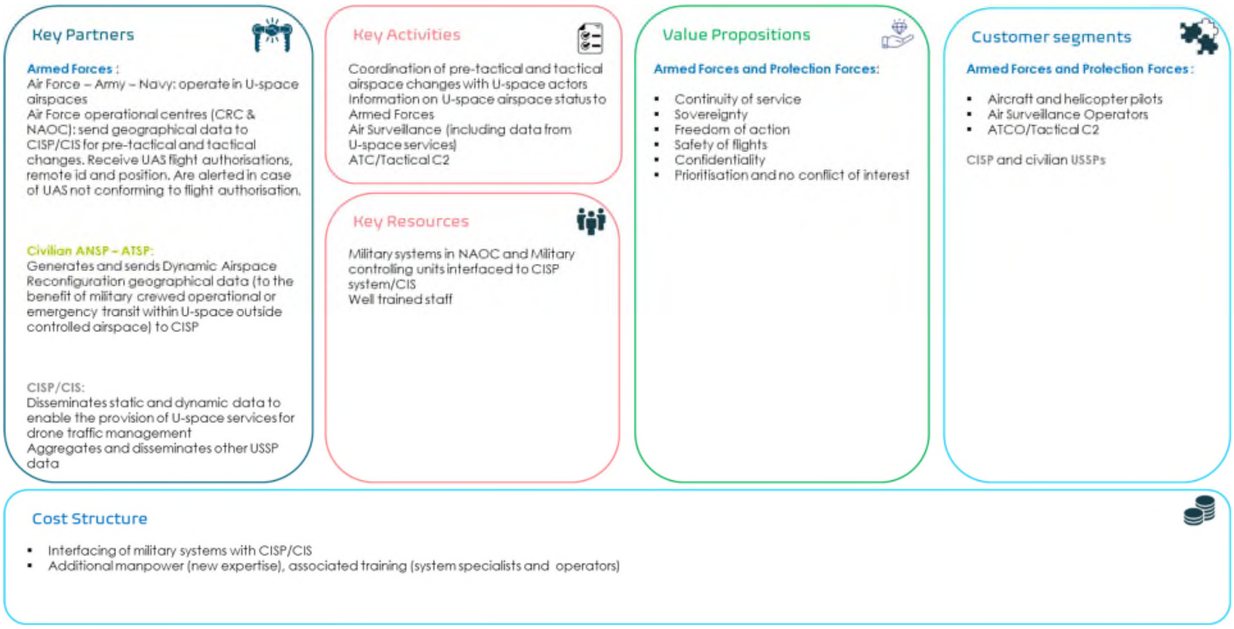
CISP and civilian USSPs

Cost Structure

- Staff training on CISP system/CIS

FIGURE 18: SIMPLIFIED BUSINESS MODEL CANVAS (SCENARIO 0)

In **Scenario 1**, and in addition to the capabilities provided in **Scenario 0**, military systems in NAOCs, CRCs and military controlling units consume U-space services, allowing military operators to receive information on drone flights within U-space airspaces. This improves the RAP, as well as the management of military manned traffic and missions. The corresponding business model is described by the following simplified canvas.



Key Partners

Armed Forces :
Air Force – Army – Navy: operate in U-space airspaces
Air Force operational centres (CRC & NAOC): send geographical data to CISP/CIS for pre-tactical and tactical changes. Receive UAS flight authorisations, remote id and position. Are alerted in case of UAS not conforming to flight authorisation.

Civilian ANSP – ATSP:
Generates and sends Dynamic Airspace Reconfiguration geographical data (to the benefit of military crewed operational or emergency transit within U-space outside controlled airspace) to CISP

CISP/CIS:
Disseminates static and dynamic data to enable the provision of U-space services for drone traffic management
Aggregates and disseminates other USSP data

Key Activities

Coordination of pre-tactical and tactical airspace changes with U-space actors
Information on U-space airspace status to Armed Forces
Air Surveillance (including data from U-space services)
ATC/Tactical C2

Key Resources

Military systems in NAOC and Military controlling units interfaced to CISP system/CIS
Well trained staff

Value Propositions

Armed Forces and Protection Forces:

- Continuity of service
- Sovereignty
- Freedom of action
- Safety of flights
- Confidentiality
- Prioritisation and no conflict of interest

Customer segments

Armed Forces and Protection Forces :

- Aircraft and helicopter pilots
- Air Surveillance Operators
- ATCO/Tactical C2

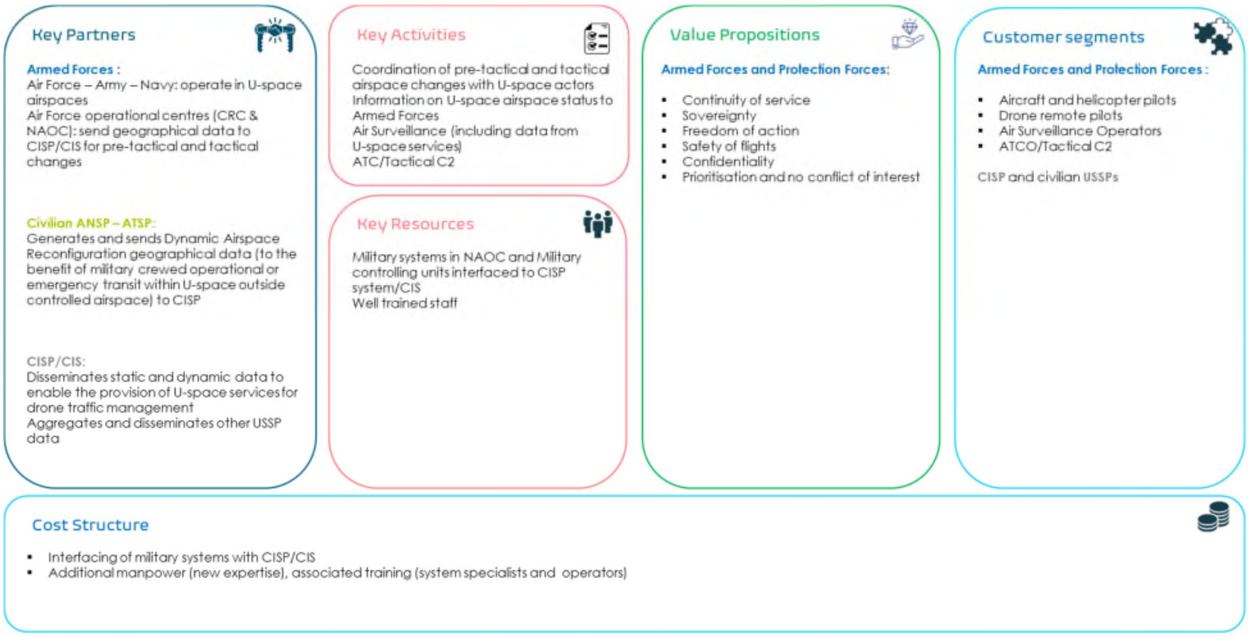
CISP and civilian USSPs

Cost Structure

- Interfacing of military systems with CISP/CIS
- Additional manpower (new expertise), associated training (system specialists and operators)

FIGURE 19: SIMPLIFIED BUSINESS MODEL CANVAS (SCENARIO 1)

In **Scenario 2**, and in addition to the capabilities provided in **Scenario 1**, military systems in NAOCs, CRCs and military controlling units provide information to the CIP/CIS, allowing U-space actors to receive information on military manned flights within U-space airspaces. This improves the safety of operations in U-space airspace for all airspace users. Military drone operators can also benefit from U-space services, allowing for a better coordination of military and civilian drone operations in U-space airspace. The corresponding business model is described by the following simplified canvas.



Key Partners

Armed Forces :
Air Force – Army – Navy: operate in U-space airspaces
Air Force operational centres (CRC & NAOC): send geographical data to CISP/CIS for pre-tactical and tactical changes

Civilian ANSP – ATSP:
Generates and sends Dynamic Airspace Reconfiguration geographical data (to the benefit of military crewed operational or emergency transit within U-space outside controlled airspace) to CISP

CISP/CIS:
Disseminates static and dynamic data to enable the provision of U-space services for drone traffic management
Aggregates and disseminates other USSP data

Key Activities

Coordination of pre-tactical and tactical airspace changes with U-space actors
Information on U-space airspace status to Armed Forces
Air Surveillance (including data from U-space services)
ATC/Tactical C2

Key Resources

Military systems in NAOC and Military controlling units interfaced to CISP system/CIS
Well trained staff

Value Propositions

Armed Forces and Protection Forces:

- Continuity of service
- Sovereignty
- Freedom of action
- Safety of flights
- Confidentiality
- Prioritisation and no conflict of interest

Customer segments

Armed Forces and Protection Forces :

- Aircraft and helicopter pilots
- Drone remote pilots
- Air Surveillance Operators
- ATCO/Tactical C2

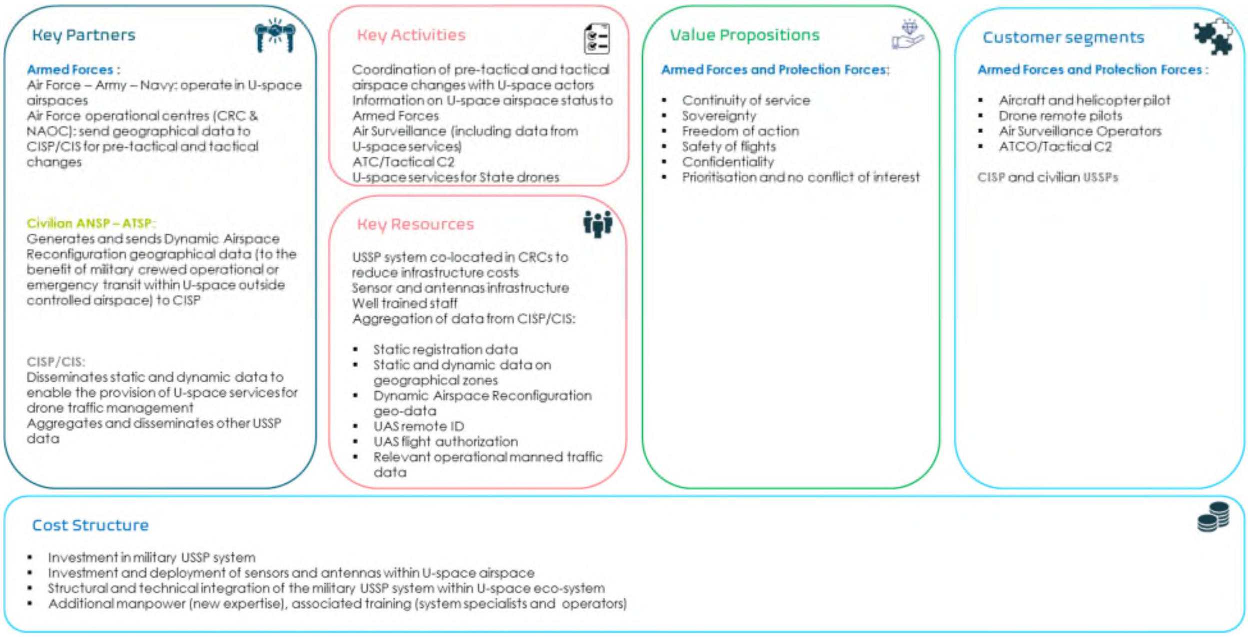
CISP and civilian USSPs

Cost Structure

- Interfacing of military systems with CISP/CIS
- Additional manpower (new expertise), associated training (system specialists and operators)

FIGURE 20: SIMPLIFIED BUSINESS MODEL (SCENARIO 2)

In **Scenarios 3** and **4**, the military would develop a USSP capability, using their own USSP system, allowing them to use the full extent of U-space services and to operate manned and unmanned assets in U-space airspace in a coordinated manner with other U-space airspace users. The corresponding business model is described by the following simplified canvas.



Key Partners

Armed Forces :
Air Force – Army – Navy: operate in U-space airspaces
Air Force operational centres (CRC & NAOC): send geographical data to CISP/CIS for pre-tactical and tactical changes

Civilian ANSP – ATSP:
Generates and sends Dynamic Airspace Reconfiguration geographical data (to the benefit of military crewed operational or emergency transit within U-space outside controlled airspace) to CISP

CISP/CIS:
Disseminates static and dynamic data to enable the provision of U-space services for drone traffic management
Aggregates and disseminates other USSP data

Key Activities

Coordination of pre-tactical and tactical airspace changes with U-space actors
Information on U-space airspace status to Armed Forces
Air Surveillance (including data from U-space services)
ATC/Tactical C2
U-space services for State drones

Key Resources

USSP system co-located in CRCs to reduce infrastructure costs
Sensor and antennas infrastructure
Well trained staff
Aggregation of data from CISP/CIS:

- Static registration data
- Static and dynamic data on geographical zones
- Dynamic Airspace Reconfiguration geo-data
- UAS remote ID
- UAS flight authorization
- Relevant operational manned traffic data

Value Propositions

Armed Forces and Protection Forces:

- Continuity of service
- Sovereignty
- Freedom of action
- Safety of flights
- Confidentiality
- Prioritisation and no conflict of interest

Customer segments

Armed Forces and Protection Forces :

- Aircraft and helicopter pilot
- Drone remote pilots
- Air Surveillance Operators
- ATCO/Tactical C2

CISP and civilian USSPs

Cost Structure

- Investment in military USSP system
- Investment and deployment of sensors and antennas within U-space airspace
- Structural and technical integration of the military USSP system within U-space eco-system
- Additional manpower (new expertise), associated training (system specialists and operators)

FIGURE 21: SIMPLIFIED BUSINESS MODEL CANVAS (SCENARIOS 3 & 4)

As illustrated through the different business models detailed above, the value propositions are identical from one scenario to another. However, the more military are integrated with U-space, the more this integration supports the military in their aviation operations, both manned and unmanned, and the more airspace users benefit from the information thus made accessible.

6 - ASSESSMENT OF IMPACT ON MILITARY SYSTEM INTERFACES

6.1 - Needs for new exchanges of information

6.1.1 - Information standards

At a technical level, any military USSP system should be able to process the U-space service data in accordance with the following standards and Service Interface Profiles, which are identified as Acceptable Means of Compliance in the U-space regulatory framework:

DATA TYPE		ORIGIN	STANDARD
	Static registration data	CAA	No standard specified
Geographical data	Static and dynamic data on geographical zones	AIS	EUROCAE ED-269 & ED-318
	Dynamic airspace reconfiguration geo-data	ATSP / NAOC	EUROCAE ED-269 & ED-318
UAS data	UAS Remote ID	USSP via CISP	ASTM F3411-22A Annex 4
	UAS Flight authorization	USSP via CISP	ASTM F3548-21

TABLE 1: APPLICABLE STANDARDS FOR U-SPACE SERVICES

The two standards that deal with geographical data are EUROCAE ED-269 and ED-318:

- The data model and interface protocol are described in EUROCAE ED-269 "Minimum Operational Performance Standard for Geofencing" ([12]): §8, §9 and App.2. ED-269 supports the delivery of the UAS geographical zone information to UAS and users, independently of the way this information is developed and maintained, in accordance with requirements on UAS geographical zones from IR (EU) 2019/947.
- The technical specification for data provision and exchange are described in EUROCAE ED-318 "Technical Specification for Geographical Zones and U-space Data Provision and Exchange" ([13]). Notably, ED-318 is a means of compliance with the geographical data requirements set forth in Article 5.1 of IR (EU) 2021/664 ([5]), regarding the static and dynamic geographical limits of U-space airspaces.

Two standards are accepted as means of compliance for the provision of UAS data associated with U-space services:

- The performance requirements for the remote identification (Remote ID) of UAS are defined in F3411-22a "Standard Specification for Remote ID and Tracking" ([14]), Annex 4. This specification defines message formats, transmission methods, and minimum performance standards for two forms of Remote ID: broadcast and network.
- Information exchanges for strategic aspects of UAS operations are covered by F3548-21 "Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability" ([15]). This document covers strategic conflict detection, aggregate conformance of operations to their operational intents, constraint awareness, and situational awareness in the event of nonconforming or contingent operations, including flight authorisation requests and provision.

6.1.2 - Exchanged information depending on operation scenarios

Depending on scenarios in section 4.1 - , the data to be exchanged is:

- Scenario 0 “UAS geographical zone manager”:
  - the national Airspace Management Cell (AMC) provides the CISP with static data and activation periods (AIP, SupAIP, NOTAM), as well as geographical data issued from neutralization or DAR’s
  - the military, as any other CISP client, gets information about UAS zones from the CISP
- Scenario 1 “consumer of U-space services” (on top of scenario 0):
  - Air Surveillance Operators get UAS remote ID to detect, track, and identify drones in the U-space airspace;
  - Military controlling units get UAS Flight authorizations to correlate drone tracks and inform military controllers about the path and intent of drone pilots, and non-conformance alerts
- Scenario 2 “consumer and provider of information to CIS” (on top of scenario 1)
  - Military controlling units provide with positioning data of manned military aircraft operating/transiting in U-space airspace, in order to compensate for the absence of e conspicuity capabilities
- Scenario 3 “national military USSP” (on top of scenario 2)
  - The military USSP provides the real-time position data of the airborne UAS with other stakeholders (USSPs, UAS operators) via the single CISP
- Scenario 4 “pan-European military USSP” does not need new kind of information to be exchanged, but the consumers and providers of these data are more numerous as the military USSP deals with several sCISP.

6.1.3 - Data from CISP to the military

6.1.3.1 - Airspace data and U-space service providers

The CISP disseminates the following static and dynamic data related to U-space zones and providers:

- Horizontal and vertical limits of the U-space airspace;
- Requirements determined for each U-space airspace:
  - UAS capabilities and performance requirements;
  - U-space services performance requirements;
  - Applicable operational conditions and airspace constraints.
- List of certified U-space service providers offering U-space services in the U-space airspace, with the following information:
  - Identification and contact details of active U-space service providers;
  - U-space services provided;
  - Certification limitation(s), if any;
- Any adjacent U-space airspace(s);
- UAS geographical zones relevant to the U-space airspace;
- Static and dynamic airspace restrictions defined by the relevant military and civil aviation authorities and permanently or temporarily limiting the volume of airspace within the U-space airspace where UAS operations can take place

6.1.3.2 - UAS data (network identification service)

As described in IR 2021/664, the CISP disseminates the following dynamic data related to UAS:

- UAS operator registration number;
- Serial number of the unmanned aircraft;
- Geographical position of the UAS;

- Altitude of the UAS above mean sea level, and height above surface or take-off point;
- Route (clockwise from true north) and ground speed of the UAS;
- Geographical position of the remote pilot, or, if not available, the take-off point;
- Emergency status of the UAS;
- Time at which the messages were generated.

This data is updated at a frequency that the competent authority has determined

6.1.4 - Data from the military to CISP

A mil USSP provides data in accordance with the services it offers:

- Network identification: provides the identity of Unmanned Aircraft System (UAS) operators and the location and trajectory of drones during operations;
- Geo-awareness: provides operators with information on operational conditions, airspace limitations or existing time restrictions, as well as creation and activation of Emergency Transit Corridors;
- Traffic information: alerts operators of air traffic that may be found near the aircraft;
- UAS flight authorization ensures free-of-conflict operations with other UAS operating in the same volume of airspace;
- Conformance monitoring (supporting service): warns of non-compliance with the granted flight clearance and informs operators of any deviation from it;

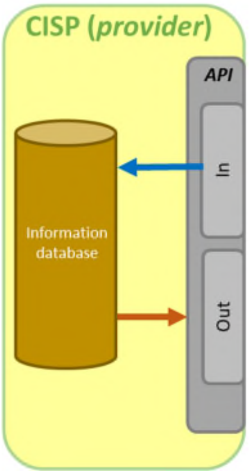
Data are the same as described in the previous section.

6.2 - High-level target architecture(s)

This chapter proposes, and describes in a formal manner, the technical architecture for the overall military ATM system and U-space systems, and how they will interface with each other. As the way military systems are implemented may vary from one MS to another, this description will be limited to major components of the systems.

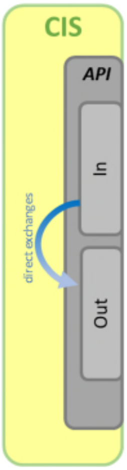
6.2.1 - Architecture options to implement CIS

As mentioned earlier (cf. 2.1.1 -), the U-space regulatory framework allows two models to implement the Common Information Services (CIS):



Centralised model:

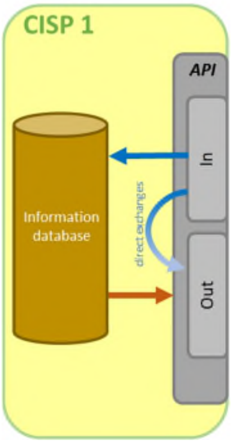
an entity is designated as the single CIS provider (CISP), and the USSPs are considered as clients of this entity.



Distributed model:

no specific entity plays a service provider role. In this case only a common address is set to support the exchange between the USSPs that all endorse both the role of providing part of the CIS and the role of consumer of services provided by others.

In the following diagrams, both options are possible. To avoid dedicating one diagram per option per scenario, the CIS will be displayed as follows, which means that both options are possible in each scenario :



The CISP in the Centralised Model may be specific to one U-space, or (more probably) shared between several U-spaces at regional or national level. This does not sensibly affect data exchanges and services provision.

6.2.2 - Scenario 0: UAS geographical zone manager

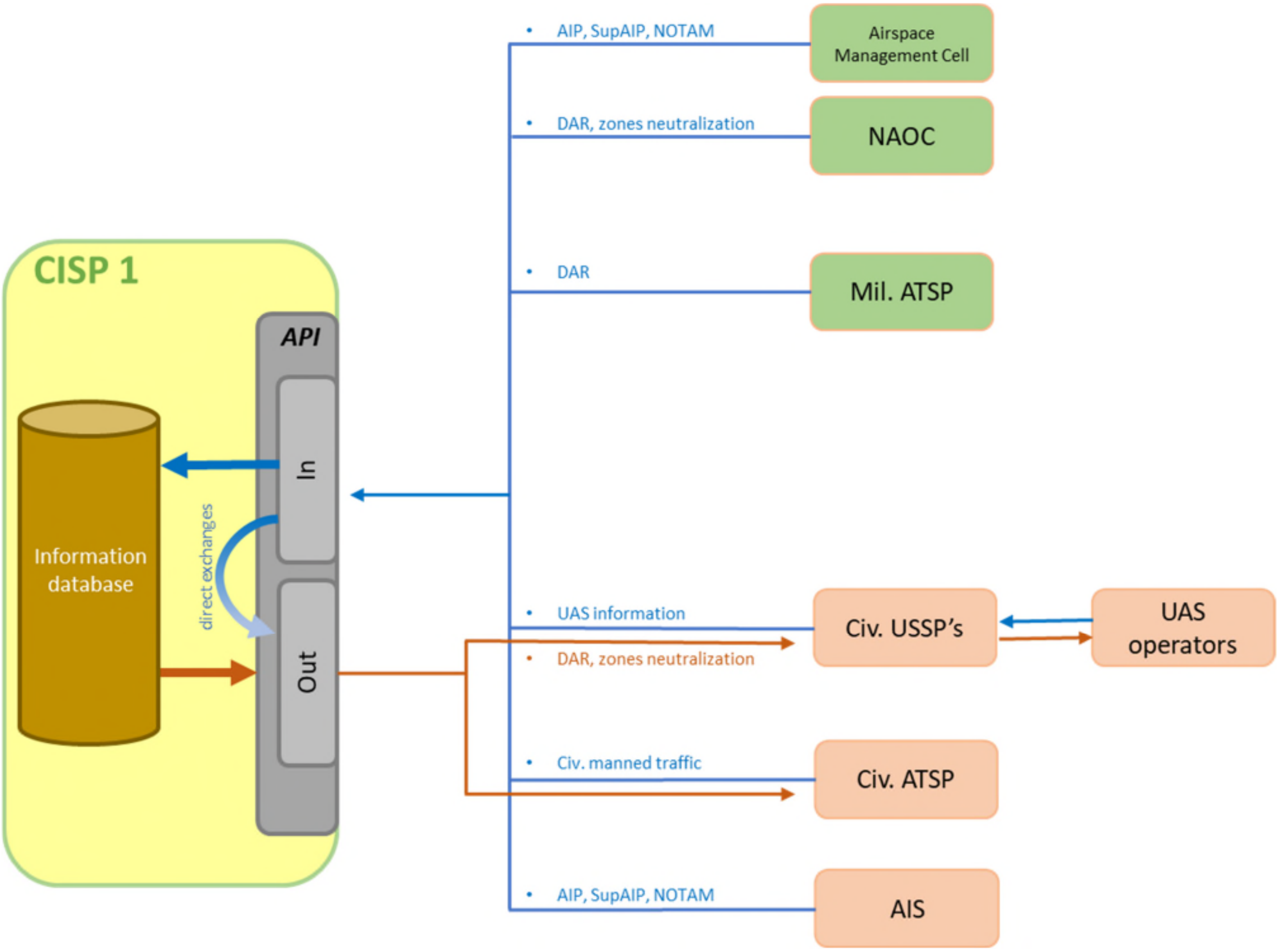


FIGURE 22: DATA EXCHANGES BETWEEN U-SPACE STAKEHOLDERS (SCENARIO 0)

As a data originator, the military provide geo-awareness and DAR data to the CISP for further dissemination. On the other hand, as the CISP centralizes geo data provided by other originators, the military may find interest in getting UAS Zones information and thus be considered as data consumers by the CISP (this does not appear in the above diagram as the data are static ones).

<u>Data originator</u>: from a strategic point of view, the national Airspace Management Cell (AMC) provides the CISP with static geo-awareness data (AIP, SupAIP, NOTAM) as it does today towards the national civilian Airspace Management system.

From a pre-tactical point of view, the military AMC, possibly a U-space dedicated section of it, disseminates day-to-day activation periods of UAS geographical areas to CISP.

Requirements for data origination are covered by the applicable rgulations, standards and best practices for the data content itself.

Data consumer: as any CISP client, the military that are interested in any particular UAS Zone shall use the interfaces that are documented in EUROCAE ED-269 standard document.

As a data consumer, the military shall use the **Retrieval Interface** to synchronously get all UAS Zone information available, and the **Subscription Interface** in order to asynchronously receive changes to UAS Zone information thanks to the **Publication Interface**.

The **Retrieval Interface** and the **Subscription Interface** conforms with SWIM TI YP (EUROCONTROL) specification that provides requirements for the transport of information using the http protocol over TLS, which ensures integrity and confidentiality.

The **Publication Interface** conforms with the AMQP Messaging specification described in the SWIM TI YP (EUROCONTROL) specification. The Publication Interface requires a network that conforms to the "IPv4 unicast" network interface binding specification, which ensures the reliability of the information exchange. All operations in this interface follow a "One Way/Fire and Forget" message exchange pattern.

6.2.3 - Scenario 1: consumer of U-space services

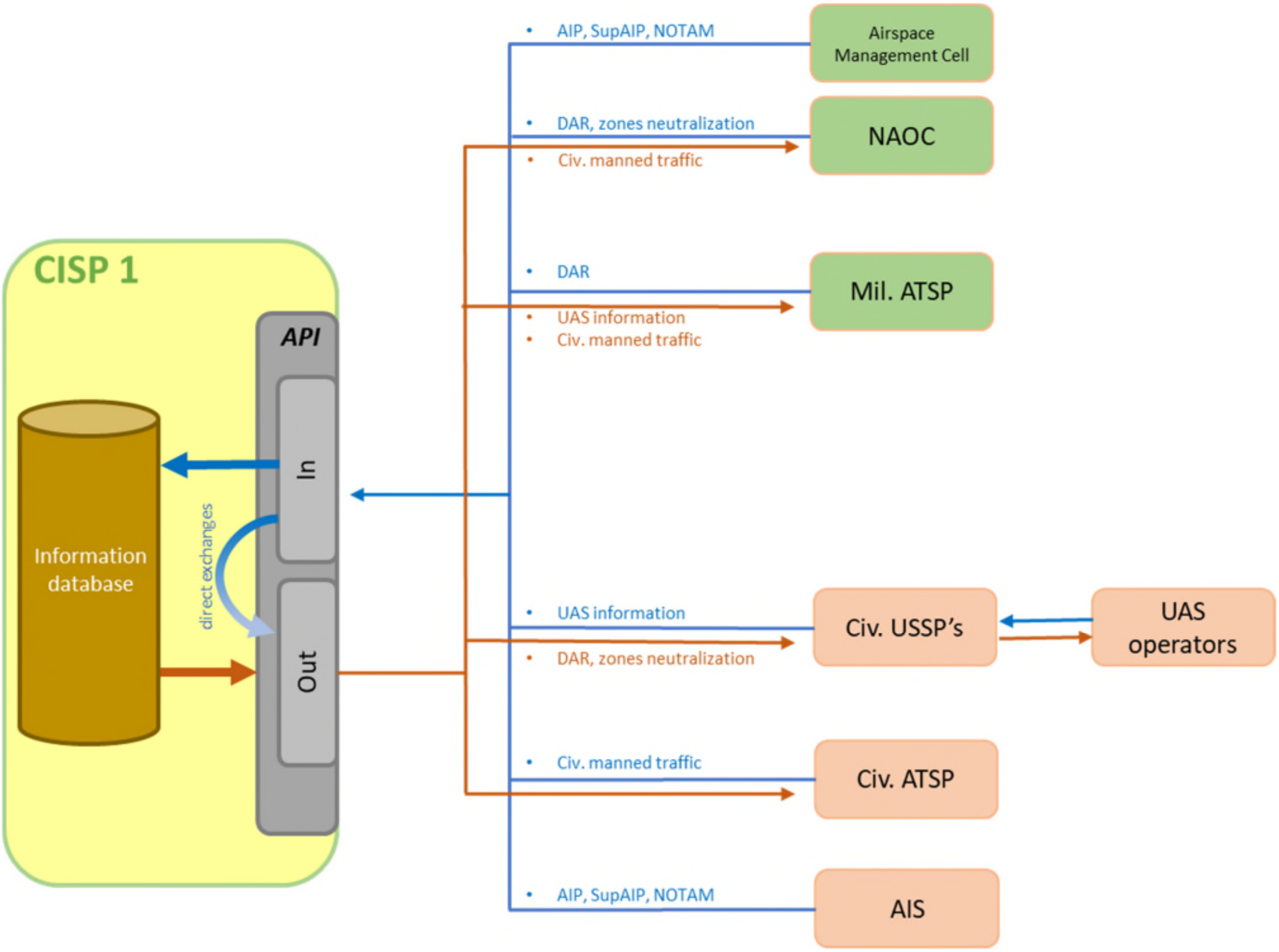


FIGURE 23: DATA EXCHANGES BETWEEN U-SPACE STAKEHOLDERS (SCENARIO 1)

In this scenario, the military is a consumer of three U-space services:

The **Network identification service** (NIS) enables Air Surveillance Operators to detect, track, and identify drones in the U-space airspace

The **UAS Flight Authorization service** allows Air Surveillance Operators to correlate drone tracks to flight authorisations, thereby more easily identifying drone flights. Tactical Controllers will have greater awareness of the path and intent of drone pilots.

The **Conformance monitoring service** provide military ATCO's with non-conformance alerts whenever an UAS does not comply with its flight plan. In case a DAR is in place, it also helps the military ATCO to monitor the airspace in order to ensure no unauthorized drone traffic penetrates any restricted airspace

6.2.4 - Scenario 2: consumer and provider of information to CIS

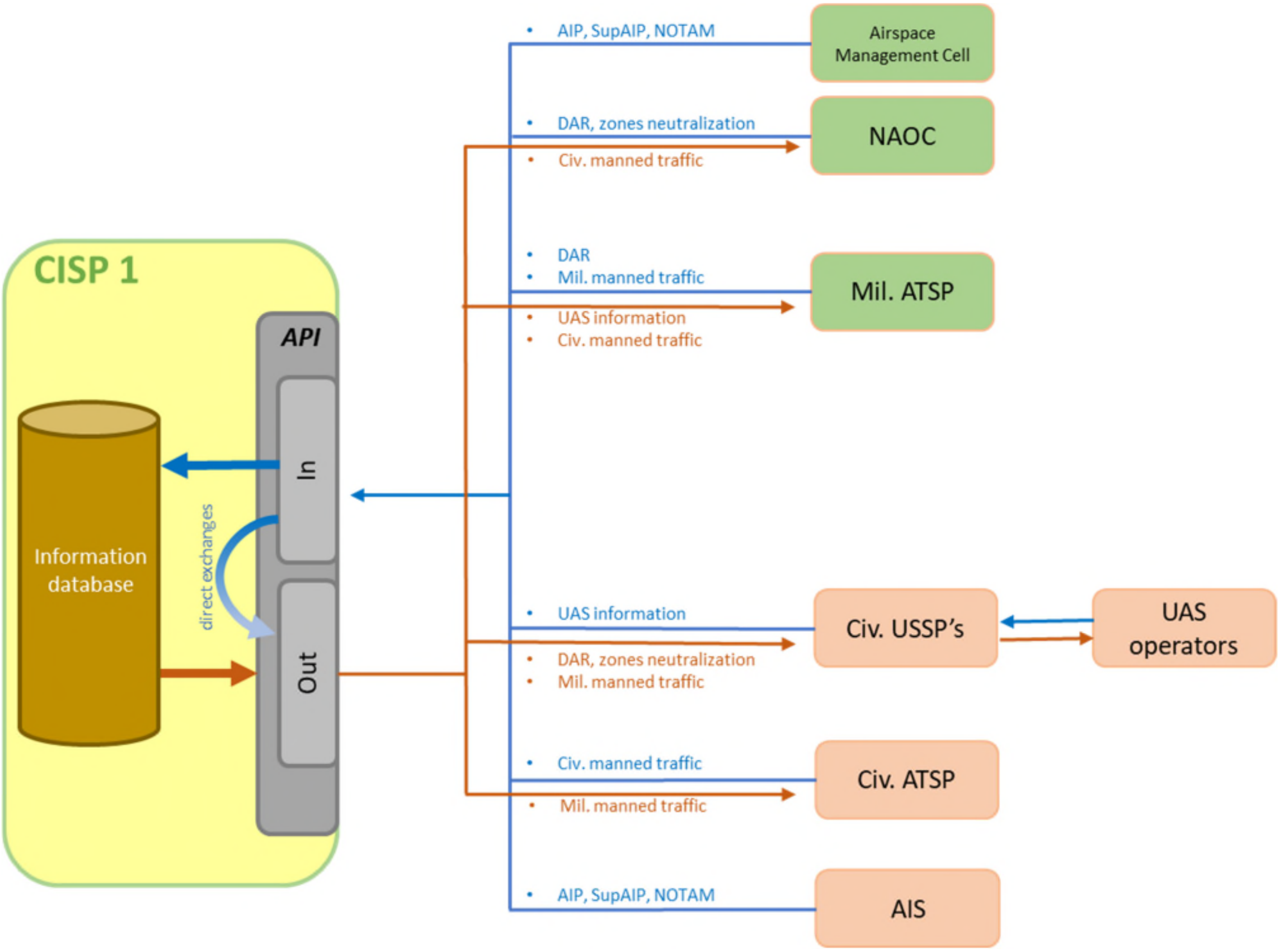


FIGURE 24: DATA EXCHANGES BETWEEN U-SPACE STAKEHOLDERS (SCENARIO 2)

In this scenario, the military provide military-specific information to U-space via the CISP. Such data could include positioning data of military aircraft operating/transiting in U-space airspace, thus compensating for the absence of e-conspicuity capabilities in an uncontrolled airspace.

6.2.5 - Scenario 3: national military USSP

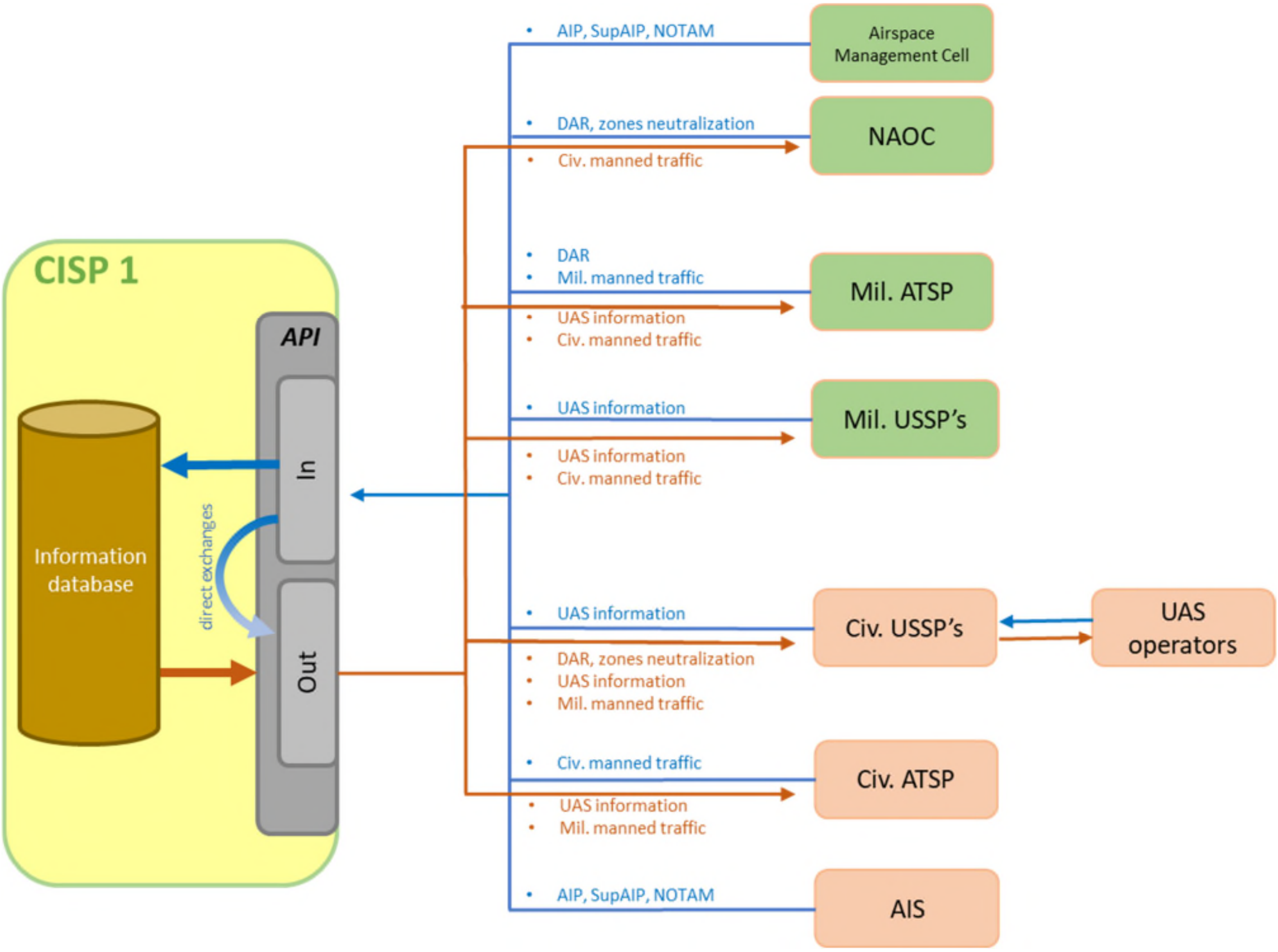


FIGURE 25: DATA EXCHANGES BETWEEN U-SPACE STAKEHOLDERS (SCENARIO 3)

The military assume the role of USSP in order to provide U-space services (5 mandatory and 2 optional) relying on digitalisation and automation of functions designed to support a safe, secure and efficient access to U-space airspace for a large number of UAS, especially considering U-space airspace configuration.

The U-space services supplied by the air force USSP might be provided to all UASs or to state drones (military, force protection, public services) only.

6.2.6 - Scenario 4: pan-European military USSP

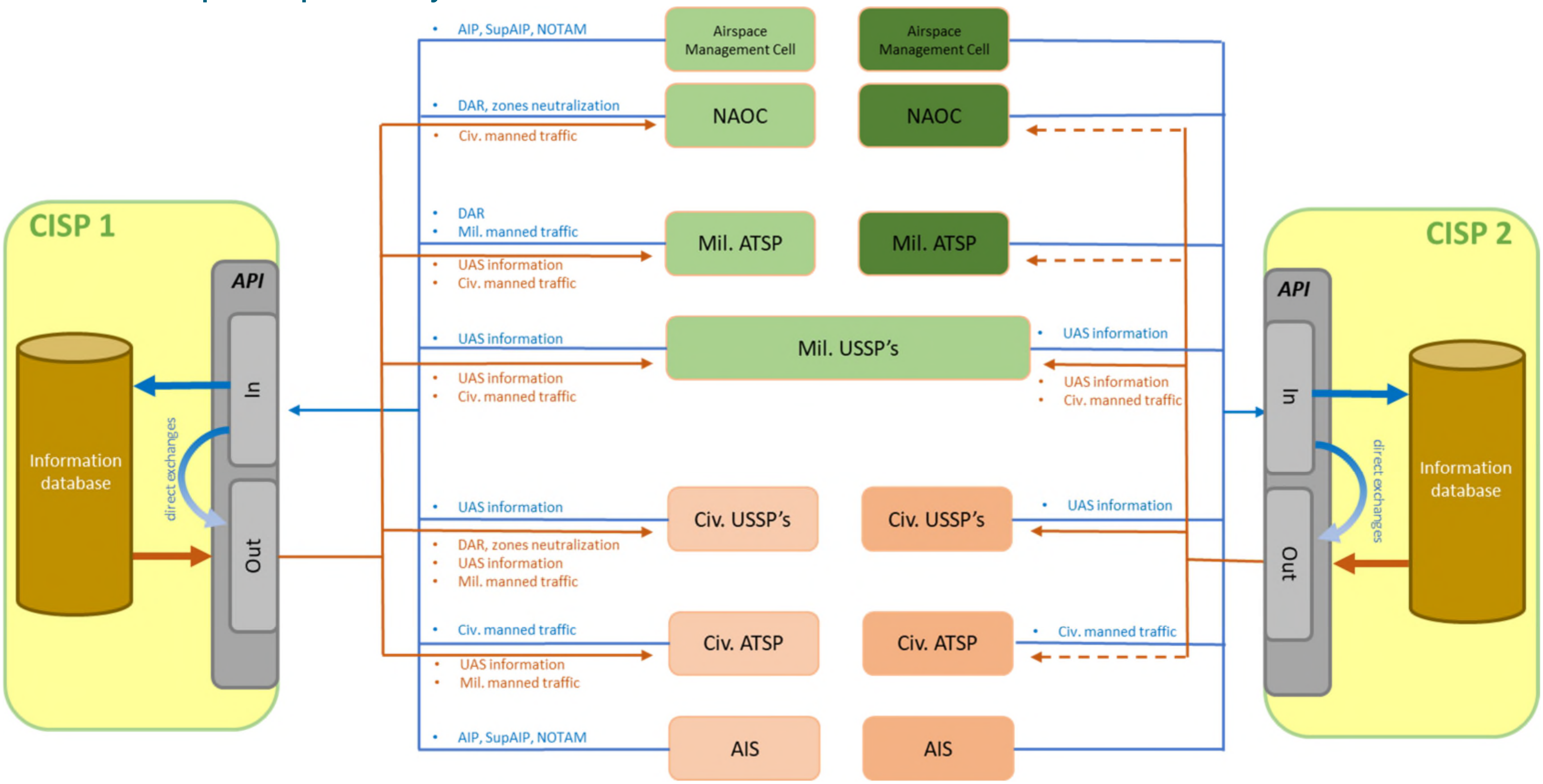


FIGURE 26: DATA EXCHANGES BETWEEN U-SPACE STAKEHOLDERS (SCENARIO 4)

An organisation of a pan-European military USSP could only be based on homogeneity of military USSP systems and delegation of responsibility and sovereignty. For cross-border operations, the USSP shall have two communication links with national single CISPs in order to share the data.

The pan-European military USSP shall deal with a potential heterogeneity of architecture options : the operational scenarios may be different, leading to different data and services to provide, and the CIS architecture option may also be different. This potential heterogeneity may lead to a high complexity implementation.

A single European CISP entity would be able to tackle such challenges with a minimum duplication of data/communication links.

7 - FINANCIAL ASSESSMENT

7.1 - Identification of costs

In order to implement the airspace management approach defined in the previous section, investments will be required in a number of areas which are detailed in this section. It is assumed that the costs would be roughly the same for all Member State. As such, distinguishing Member State for costs would not be relevant in this case.

Pending validation and refinement with the project stakeholders, the cost of capital for the militaries is assumed to be 4%, i.e. 2.5% for Time Value of Money (TVM) plus a 1.5% Premium Risk. The inflation rate is estimated at 3% for the time period. According to the European Central Bank, inflation rate should stabilize around 2% overall for the following years but services have a much higher inflation (around 3.7% in May 2024) hence the value of 3% has been kept. The resulting discount rate would be 7.1% (TVM plus Premium Risk and multiplied by inflation) for the time period.

7.1.1 - IT implementation

The information systems needed by the military to implement the operational scenarios detailed in section 4 - include operator workstations and connectivity to a communication network. In case the military would take on a role as USSP, they would also have to invest in servers or data centres.

In deliverable D2 (Cost benefit analysis) of the SC1 of the "Military and U-space: guidelines" study, the costs of a workstation is estimated to be €10.000 and would have to be renewed every 10 years (estimated lifetime of the workstation's hardware). This amount has to be multiplied by the number of operators performing coordination with USSPs, which depends on the local organisation (see also 7.1.4 -).

7.1.1.1 - Scenario 0: UAS geographical zone manager

In this scenario, mostly new procedures supporting Dynamic Airspace Reconfiguration should be implemented to coordinate between the NAOC/military controlling unit and the CISP/CIS. IT implementations are limited to connectivity to a communication network, so allow sending geographical data in real time.

7.1.1.2 - Scenario 1: consumer of U-space services

Compared with scenario 0, the NAOC/military controlling unit should have the IT infrastructure and procedures to receive and consume U-space services. Mostly new communication and exchange systems are required combined with updated procedures.

7.1.1.3 - Scenario 2: consumer and provider of information to CIS

In this scenario, the NAOC/military controlling unit should expand its communication and system capabilities to be able to provide military U-space information from their workstations to the associated CISP/CIS.

7.1.1.4 - Scenario 3: national military USSP

While the NAOC/military controlling unit would retain its capabilities to consume and provide U-space information, this scenario features the development of a national military USSP. Such implementation will require new systems, staff and operational costs. The military would have to develop/commission a new USSP system and its associated workstations, servers, HMIs and staff. It is assumed that a national USSP would be located within the NAOC, hence no rental or construction costs are associated with this scenario.

7.1.1.5 - Scenario 4: pan-European military USSP

This scenario is similar to scenario 3 with the difference that a single military USSP would be implemented for all EDA Member States. The costs of deploying a pan-European USSP would not be significantly different from those of a national USSP except for servers/data and support staff. This USSP could be attached to a Member state's NAOC, resulting in no additional rental or construction costs.

7.1.2 - Process implementation

The review and update of U-space related processes to implement the operational scenarios under consideration may involve various operational and non-operational stakeholders of the Member States' military organisations and their interaction with external stakeholders. Depending on the organisational structure and existing processes in place, the implementation of changes can vary significantly between Member States and the scope of the processes in question.

The military would incur costs at national level to define the detailed processes required for airspace management and implement them into their operations, and then to propagate this information to military operational units. There is no strong variation between the different scenarios. Scenarios 0 and 1 would have minimal communication processes allowing an ATS unit or CRC to communicate with a CISP/USSP, with scenario 0 not requiring to develop process permitting an ATS unit or CRC to receive information from a CISP/USSP.

7.1.3 - Implementation studies

Each Member State is assumed to need a detailed study about the implications for the military of implementing the proposed operational scenario. The study would reiterate the scope of the corresponding operational concept, applying specific and detailed inputs applicable to the Member State. The scope of the study would encompass strategic, economic, operational as well as detailed technical questions concerning the required system upgrades IT related issues.

The corresponding costs are estimated to be about 25% of those of a full U-space implementation, as envisaged in SC1's D2. This would amount to €250k€ for all scenarios.

7.1.4 - Staff training and documentation

The costs of updating training material and other documentation are expected to vary depending on the Member State and the number of staff to be trained, the size of the affected military organisations, the number of operational units involved, etc. At the level of the operator, the scope and frequency of the coordination tasks described in section 4 - is probably sufficiently low to not require recurring training, so only initial training is considered here. For other scenarios

The corresponding are estimated to be about 25% of those of a full U-space implementation, as envisaged in SC1's D2. So costs related to training material and documentation would amount to €100k per MS and there will be no costs related to initial training activities since these trainings will be supervised by military personnel.

Only in scenarios 3 and 4, when implementing the military USSP as a new operational unit, would additional staff become necessary. The new staff would comprise a unit commander (with possibly an assistant), sixteen technicians dedicated to support and development, and two managers to supervise them.

7.1.5 - Office space

As the hardware required to implement the airspace management concept detailed in section 4 - is very limited, the impact on office space is considered to be negligible for the purpose of this cost assessment. However, costs of office accommodation will occur and will depend on the number of extra personnel required in the national implementation. The same would apply to a national USSP which will probably be deployed in an existing CRC (Control and Reporting Center) or NAOC, resulting in no office space costs.

7.1.6 - Utilities

The cost for data subscriptions and data links into the premises of the CISP/USSP is estimated to be of €10,000 per year and per operational unit coordinating with U-space. The cost of license fees for system updates is estimated at €100k per year. In Scenario 4, the cost of data subscription is expected to scale with the number of countries, leading to a total cost of € 270k for all EDA members.

7.1.7 - Cost summary

The following table provide a summary of the above costs, per area.

Cost area	Category	Amount	Details
IT implementation	Visualisation of data CISP/USSP to ATS	€10k per CRC	1 workstation
	Data exchange ATS to CISP/USSP	€200k per Member State	2 full-time equivalent (FTE)
	Data exchange CISP/USSP to ATS	€200k per Member State	2 FTE
	Mitigation of cyber security risks	€100k per Member State	1 FTE
	Data interface USSP	€100k per Member State	1 FTE
	Data interface for ATM surveillance data	€100k per Member State	1 FTE
	USSP server	€75k per USSP	3 servers
	USSP system	€1,100k per USSP	1 system
	USSP workstation	€30k per USSP	3 workstations
	USSP implementation	€200k per USSP	2 FTE
Process implementation	Strategic/pre-tactical airspace management coordination	€50k per Member State	
	Propagation of strategic/pre-tactical information to operational units	€100k per Member State	
	Military ATS unit communicates to CISP/USSP	€100k per Member State	
	Military ATS receive information from CISP/USSP	€100k per Member State	
Training and documentation	Update of training materials and manuals	€100k per Member State	
Utilities		€10.000 per operational unit	
Implementation studies	Studies	€250k per Member State	

TABLE 2: OVERVIEW OF U-SPACE-RELATED COSTS FOR THE MILITARY

7.1.7.1 - Scenario 0: UAS geographical zone manager

A more detailed breakdown of the expenditure categories for scenario 0 shows that in the case where the militaries only commit to a minimal level of collaboration, the biggest single cost item would be to conduct initial studies to fully understand the ramifications of U-space implementation at national level (€ 250k). This is necessary to ensure all safety critical and security related risks can be identified and mitigated. Furthermore, minimal IT implementation would be required for the ATS unit/CRC to communicate with the CISP/CIS (€ 100k) paired with mitigation of cyber-security risks (€ 50k) associated with such communications. The processes involving the strategic and pre-tactical airspace management and information need to be revised and adjusted

(€ 150k), followed by minor updates in the training syllabus and manuals for affected staff (€ 100k) and new procedures to allow the military ATS unit/CRC to communicate with the CISP/CIS(50k).

The non-discounted capital expenditure for this scenario is € -700k for a given Member State, while the discounted capital expenditure for this scenario is € -545k.

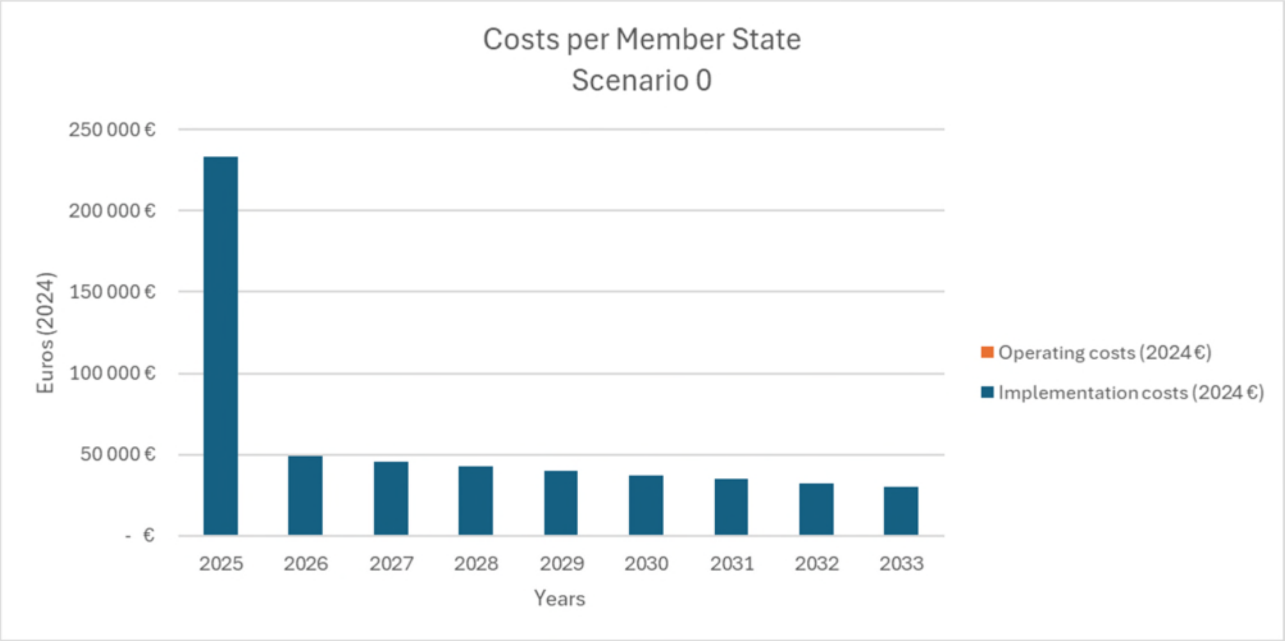


FIGURE 27: COSTS PER MEMBER STATE IN 2024 EUROS – SCENARIO 0

7.1.7.2 - Scenario 1: consumer of U-space services

For Scenario 1, all previous costs from Scenario 0 still apply. However, to consume U-space services, the military ATS unit/CRC should develop and implement visualisation systems (€ 200k) and provide additional workstations (€ 20k). Furthermore, communication systems allowing a CISP/CIS to communicate with the ATS unit/CRC should be developed and implemented (€ 200k). Due to the addition of these systems, cyber-security risks mitigation will increase its costs (from € 50k in Scenario 0 to € 100k in Scenario 1). Finally new processes should be developed to ensure that the ATS unit/CRC receives information from the CISP/CIS (€ 100k).

The non-discounted capital expenditure for this scenario is € -1.27 million per Member State, while the discounted capital expenditure for this scenario is € -941k.

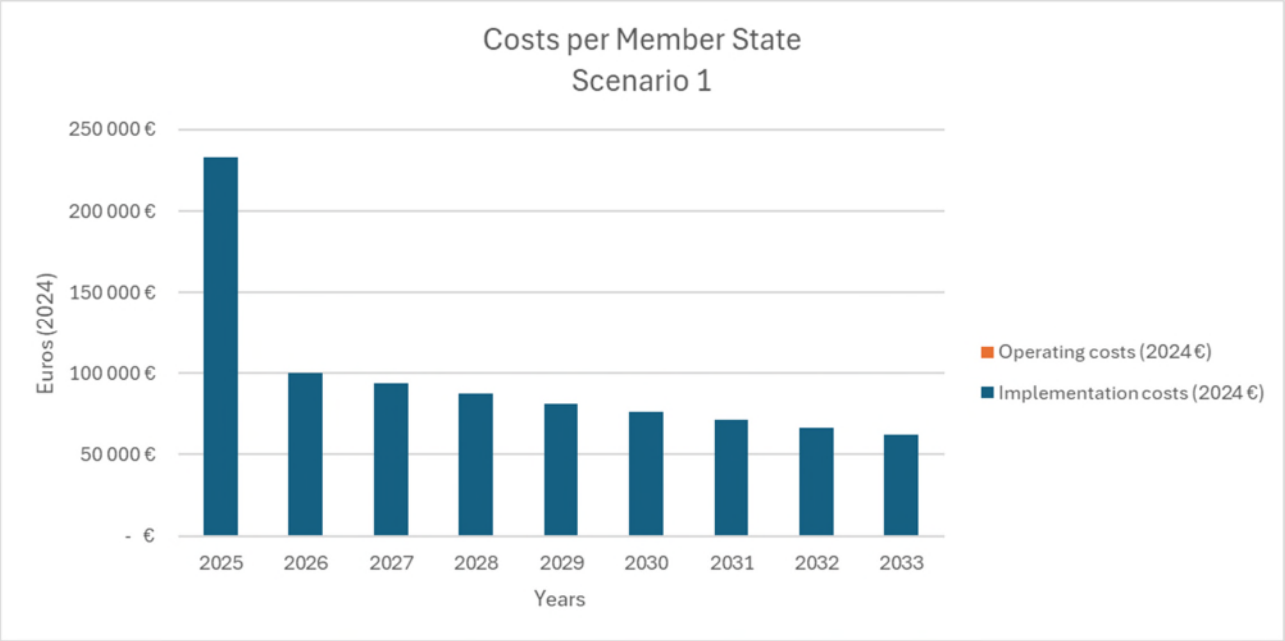


FIGURE 28: COSTS PER MEMBER STATE IN 2024 EUROS – SCENARIO 1

7.1.7.3 - Scenario 2: consumer and provider of information to CIS

For Scenario 2, all previous costs from Scenario 1 would still apply. However, to provide information to the CISP/CIS, the military ATS unit/CRC would have to expand its communication system with the capability to provide ATS information to the CISP/CIS (from € 100k in Scenario 0 to € 200k in Scenario 2), paired with an expansion of associated processes (from € 50k in Scenario 0 to € 100k in Scenario 2).

The non-discounted capital expenditure for this scenario is € -1.420 million per Member State, while the discounted capital expenditure for this scenario is € -1.045 million per Member State.

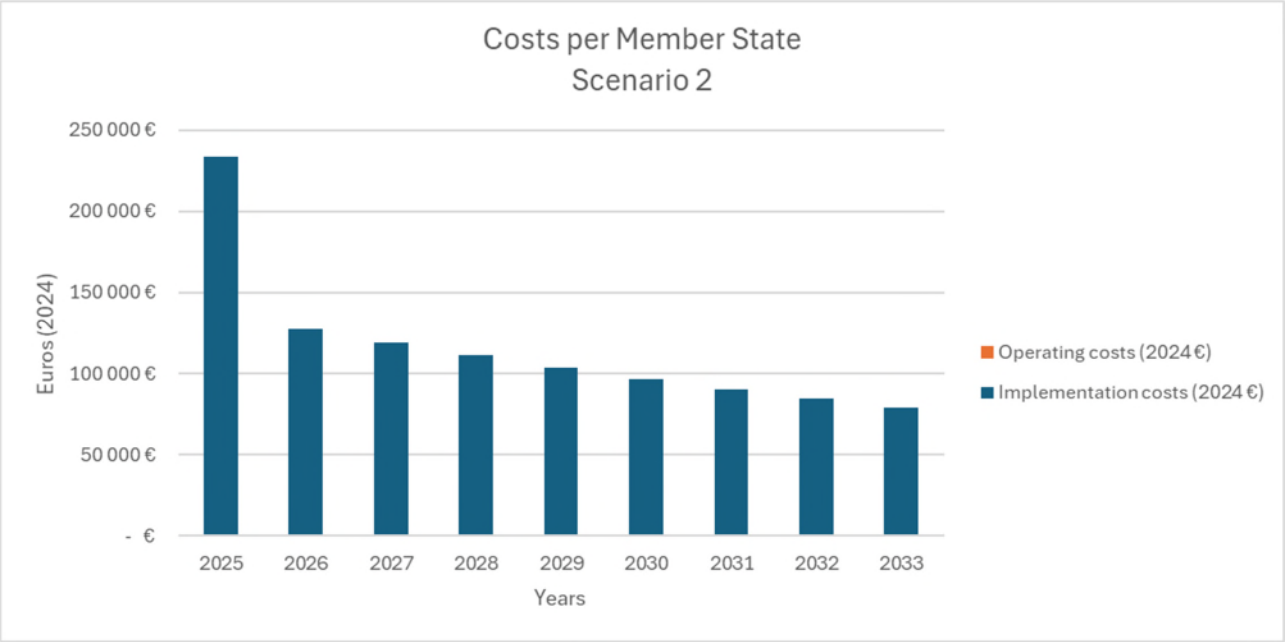


FIGURE 29: COSTS PER MEMBER STATE IN 2024 EUROS – SCENARIO 2

7.1.7.4 - Scenario 3: national military USSP

For Scenario 3, and since the military ATS unit/CRC would still communicate with the CISP/CIS, all previous costs from Scenario 2 would still apply. In this scenario, each Member State develops its own military USSP. The biggest single cost would be the definition and procurement of the USSP system itself (€ 1.1 million), followed by its implementation (€ 200k), the interface for ATM surveillance data (€ 100k) and the associated workstations (€ 15k for 3 workstations) and three servers (€ 75k).

Additionally, this military USSP should have its own staff: a unit manager (an officer of rank OF1), 2 managers (non-commissioned officers of rank OR9) and 16 technicians for support, maintenance, and development (non-commissioned officers of rank between OR6 and OR8). License fees to update the system would apply annually (€ 100k), coupled with a data subscription service (€ 10k).

The non-discounted capital expenditure and operating expenses for this scenario are € -7.042 million per Member State, while the discounted capital expenditure and operating expenses for this scenario are € -4.944 million per Member State.

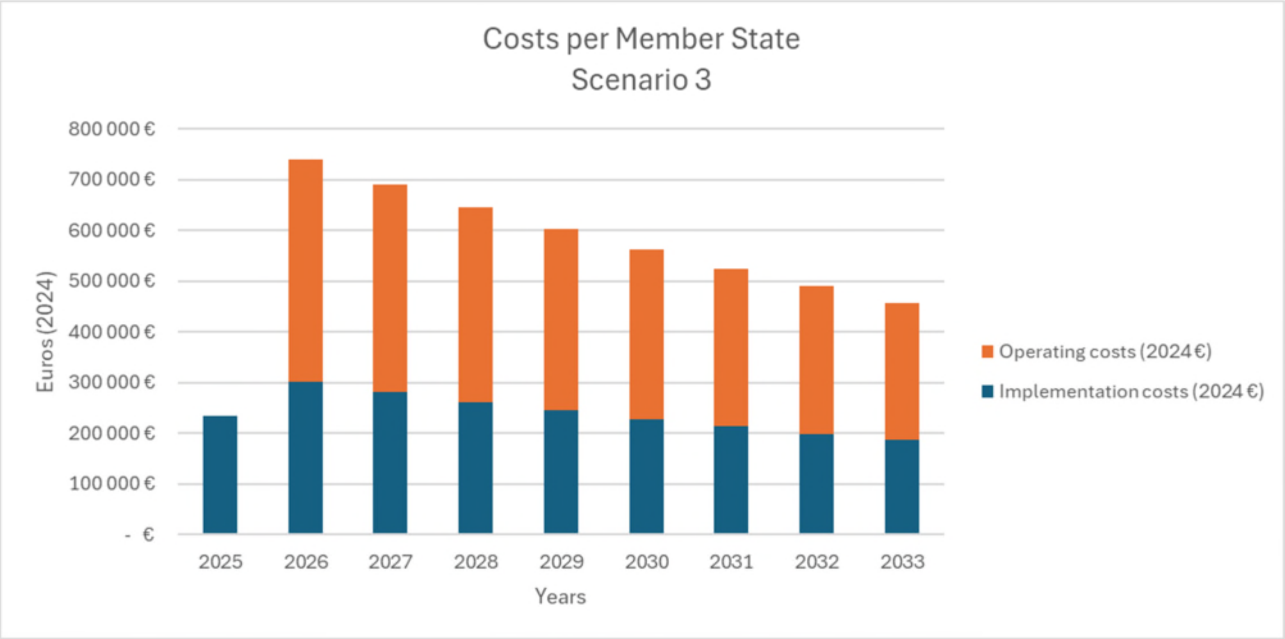


FIGURE 30: COSTS PER MEMBER STATE IN 2024 EUROS – SCENARIO 3

7.1.7.5 - Scenario 4: pan-European military USSP

For Scenario 4, there is only one USSP for all EDA Member States. Considering the needs of a USSP in terms of staff and infrastructure, it is unlikely that this USSP would have a dedicated building and would likely be hosted by the NAOC of one of the Member State.

The difference in costs compared with Scenario 3 would be in operational costs: there would be 2 unit managers instead of one (one officer of rank OF2, and one of rank OF1 to assist him) and there would be 4 managers instead of 2. It is also expected that the data subscription would scale with the number of countries covered (from € 10k in Scenario 3 to € 270k in Scenario 4).

The non-discounted capital expenditure and operating expenses for this scenario are € -9.754 million for all EDA Member States, while the discounted capital expenditure and operating expenses for this scenario are € -6.825 million for all EDA Member States.

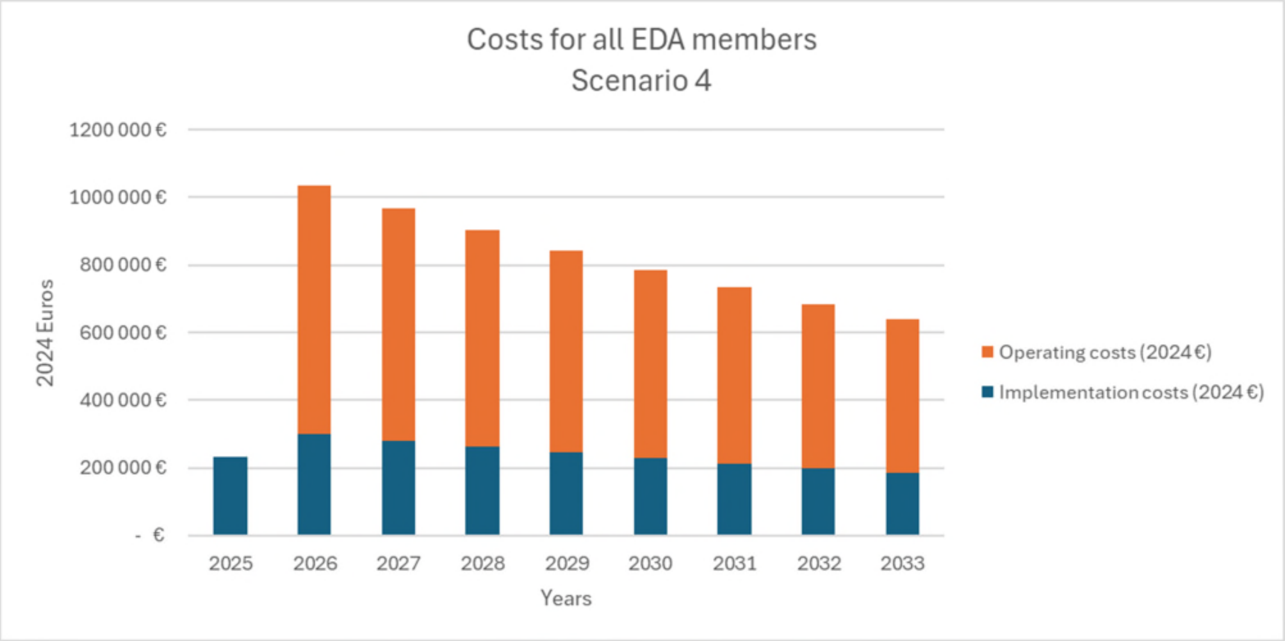


FIGURE 31: CUMULATED COSTS FOR ALL MEMBER STATES IN 2024 EUROS – SCENARIO 4

7.2 - Cost sharing

As indicated above, the information systems to implement the U-space airspace management would be provided by the USSP, and therefore, the corresponding costs would be supported by this actor, either entirely or in part.

Consequently, in order to support the integration with U-space, the military would have recurring costs related to staff costs and utilities (i.e. power, data subscriptions, data links, etc.).

A military USSP could share its implementation costs with a civilian USSP. This would depend on the willingness of military institutions to share their systems and information with civilian counterparts. Moreover, if a military USSP would be deployed in a CRC or NAOC, it may be difficult to share systems with civilians.

7.3 - Funding opportunities

SC1's deliverable D2 investigated the funding opportunities available to the military to help supporting the costs of U-space implementation. Although the costs identified above are limited and may not justify going through the process of requesting dedicated funding through national or European mechanisms, the options identified in SC1 remain valid at this stage.

8 - GUIDELINES ON A FUTURE ROLE FOR THE MILITARY IN U-SPACE

The European Defence Agency (EDA) has initiated the "Military and U-space: guidelines" study in January 2021 to assess military impacts and cost benefits of large-scale drone operations in dedicated U-space airspaces. Understanding normal/nominal operations in a U-space "eco-system" is a prerequisite for the military to collaborate in U-space concept development.

The present report presents the conclusions and recommendations of the 4th Specific Contract (SC4) carried out under the study, which investigates how the military could adopt an active role in U-space and which benefits and risks they would accrue in doing so. Various operational scenarios have been considered, ranging from the military taking on a role as UAS geographical zone manager similar to today operations, to the creation of a pan-European military USSP sharing information with the CISP/CIS of all Member States. These scenarios correspond to an increasing level of cooperation with and integration into U-space operations.

Scenario	Military role
Scenario 0	UAS geographical zone manager
Scenario 1	Consumer of U-space services
Scenario 2	Consumer and provider of information to CIS
Scenario 3	National miliatry USSP
Scenario 4	Pan-European military USSP

TABLE 3: LIST OF SCENARIOS UNDER ASSESSMENT

The SWOT analysis performed on the various operational scenarios considered in SC4 does not allow identifying one scenario with clear benefits over the others. Rather, the different scenarios correspond to increased level of integration of the military into the U-space operational processes and technical systems, which provide increasing benefits in term of mission effectiveness and safety, but at the cost of increased financial investments and cyber security risks.

Although **Scenario 4** would provide significant economies of scale, it is probably too politically complex to be implemented in the short term. For a near future objective, **Scenarios 0** to **3** are thus more realistic options, and also leave each Member State to decide on their ambition regarding the involvement of their military in U-space. The most important step toward this objective would be for the military to acquire the connectivity with the CISP/CIS; once this is achieved, the gaps between **Scenarios 1**, **2** and **3** are limited. Consequently, aiming from the start for a higher level of integration (i.e. **Scenario 2** or **Scenario 3**) would be more efficient compared to a staged approach and would deliver important benefits more rapidly.

Lastly, it is interesting to note that the different scenarios assessed in SC4 are not mutually exclusive, but rather represent the incremental steps that allow reaching a high level of military integration with U-space. Therefore, a Member State looking to implement **Scenario 3** could build a programme to that effect, which first phases would correspond to **Scenarios 1** and **2**.

The financial assessment of the different scenarios showed that **Scenarios 0** to **2** require comparable investments, in the order of 1 million euros, as they only require the military to develop new interfaces to their existing systems. On the other hand, **Scenarios 3** and **4** involve much more significant investments and operating costs (by a factor of about 10 compare to scenarios 0 to 2) as a full new operational unit, a military USSP, would be required under these scenarios.

An assessment of the organisational changes required to implement the scenarios under consideration showed that they could fit within existing organisations without requiring significant changes. Indeed, the additional staff needed for **Scenarios 0** to **2** is very limited and could be implemented by allocating new responsibilities and tasks to existing functions (ASM cell, NAOC, ATS unit, CRC). **Scenarios 3** and **4** would require the creation of a new military function (a military USSP), which implies training new staff and defining new processes, but could benefit from the similarities with civilian counterparts, which are precisely in the process of creating the CISP functions within their respective organisations.

Data sharing in the U-space environment is governed by a number of specific standards developed by EUROCAE and ASTM International. Similar standards are already used jointly by military and civilian ANSPs for information-sharing and operational coordination in ATM. Military system providers should thus be in a position to upgrade these systems at limited costs and risks, should the military decide to interface them with U-space systems. Data to be provided by the military are geographical data (for the geo-awareness services and the DAR process) and manned traffic data (for the traffic information service); U-space expect this data to be provided using formats that are already used, or under implementation, within civilian ATM. The most significant effort in terms of new interface development would be to receive data from the U-space services (network identification, UAS flight authorisation, conformance monitoring), for which there is no operational implementation in civilian ATM to date[11]. This challenge is common to **Scenarios 1** to **4**.

Based on these results achieved by SC4:

- The military are invited to consider implementing **Scenario 2** (i.e. provision of information to U-space and reception of information from U-space), before potentially evolving toward **Scenario 3** in a second step, with the creation of a military USSP function within their organisation. This military USSP may not necessarily provide exactly the same services as required from a civilian USSP by the U-space regulatory framework, but would provide through these services the capability to manage military UAS traffic, support military UAS operations and coordinate with civilian U-space stakeholders.
- Single CISPs are invited to cooperate with in the definition of a national U-space concept that takes into consideration the specific needs of the military, whether for air operations (access to the airspace, airspace management, segregation of manned and unmanned traffic, etc.) or for military missions (Air Surveillance, Air Defence, support to public services, etc.). This concept should then be refined into services based on the data that the military and the CISP decide to exchange.
- In those Member States that have decided to implement a distributed U-space architecture, with no CISP, the coordination between the military and other U-space stakeholders should be managed by the national U-space project sponsor (usually, the national Civil Aviation Authority or the Ministry of Transport). The military would have to establish coordination with all civilian USSPs for the development of the Common Information Service and the exchange of information between USSPs, in order to have their requirements taken into consideration.

[11] *This ATM-U-space interface should be implementeted,(at least for the mandatory U-space services) when the first U-space airspaces go live, tentatively in early 2025.*

9 - APPENDIX A: TERMINOLOGY

Acronym	Definition
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance – Broadcast
ADS-L	Automatic Dependent Surveillance – Light
AGL	Above Ground Level
AIP	Aeronautical Information Publication
AIRAC	Aeronautical Information Regulation and Control
AMC (regulation)	Acceptable Means of Compliance
AMC (airspace management)	Airspace Management Cell
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ARP	Aerodrome Reference Point
ASM	Airspace Management
ATSP	Air Traffic Service Provider
ATC	Air Traffic Control
ATM	Air Traffic Management
AWACS	Airborne Warning and Control System
BVLOS	Behind Visual Line Of Sight
CAT	Commercial Air Traffic
CIS	Common Information Services
CISP	Common Information Service Provider
CTR	Control Zone
DAR	Dynamic Airspace Reconfiguration
EASA	European Union Aviation Safety Agency
EDA	European Defence Agency
EET	Estimated Elapsed Time
ETSO	European Technical Standard Order
EU	European Union

Acronym	Definition
FIR	Flight Information Region
FIS-B	Flight Information Service – Broadcast
FOCA	Federal Office of Civil Aviation
GA	General Aviation
GAT	General Air Traffic
GM	Guidance Material
GNSS	Global Navigation Satellite System
HEMS	Helicopter Emergency Medical Services
HMI	Human-Machine Interface
HTA	Helicopter Training Area
ICAO	International Civil Aviation Organization
IFF	Identification Friend or Foe
ISM	Industrial, Scientific, and Medical
IR	Implementing Regulation
LFA	Low Flying Area
MEDEVAC	Medical Evacuation
MHz	Megahertz
MRVA	Minimum Radar Vectoring Altitude
MS	Member State
NAOC	National Air Operation Centre
NDZ	No Drone Zone
NM	Nautical Mile
NOTAM	Notice To Airmen
OAT	Operational Air Traffic
SAR	Search And Rescue
SC	Specific Contract
SERA	Standardised European Rules of the Air
SESAR	Single European Sky ATM Research
SRD	Short-Range Device

Acronym	Definition
TAS	True Air Speed
TC	Transit Corridor
TMA	Terminal Control Area
TRZ	Temporary Restricted Zone
TSO	Technical Standard Order
UAS	Unmanned Aircraft System
UTC	Coordinated Universal Time
USSP	U-space Service Provider
UTM	UAS Traffic Management
VFR	Visual Flight Rules
VLL	Very Low Level
VLOS	Visual Line Of Sight

10 - APPENDIX B: REFERENCES

[1] European Commission, A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe, 29 November 2022

[2] ICAO – Unmanned Aircraft Systems Traffic, Management (UTM) – A Common Framework with Core Principles for Global Harmonization, Edition 3

[3] EDA – White paper - U-space, Drones and Military Low Level Flights, April 2019

[4] SESAR JU – U-space Blueprint, 2017

[5] European Commission, U-space regulatory package (IR (EU) 2021/664, 2021/665 & 2021/666), 2021

[6] EASA, Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space
https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2022024r

[7] EDA – Military and U-space: guidelines, SC1 Final Report, 2024

[8] EDA – Military and U-space: guidelines, SC3 Final Report, 2022

[9] European Commission, Drone Strategy 2.0, 2022

[10]EASA – Technical Specification for ADS-L transmissions using SRD-860 frequency band (ADS-L 4 SRD-860)
https://www.easa.europa.eu/sites/default/files/dfu/ads-l_4_srd860_issue_1.pdf

[11]Plan de Acción Nacional para el Despliegue del U-SPACE 2022-2025, Ministerio de Transportes, Movilidad y Agenda urbana, 2022
https://cdn.mitma.gob.es/portal-web-drupal/aviacion/220208_plan_de_despliegue_u-space_vfinal_acordada.pdf

[12]EUROCAE – ED-269 – Minimum Operational Performance Standard for UAS Geo-Fencing, 2020

[13]EUROCAE – ED-318 – Technical Specification for Geographical Zones and U-Space data provision and exchange, 2024

[14]ASTM International – F3411-22a – Standard Specification for Remote ID and Tracking, 2022

[15]ASTM International – F3548-21 – Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability