Fondation pour la Recherche Stratégique

EXECUTIVE SUMMARY

Study on suitable governance and Data Policy models for a European Space Situational Awareness (SSA) System

Study Team Members:
FRS (Leader) – Xavier Pasco

Dipartimento di Ingegneria Aerospaziale e Astronautica (Sapienza)
EUTELSAT
IAI
VBL studio legale e tributario

(Agreed external expertise: ONERA – EADS Astrium – Thales Alenia Space)

Paris, June 2008
N° 288/FRS/SSA
Contract n° 21443/08/F/MOS
European Space Agency

1 – Introduction

Europe's dependence on space assets has increased over the years. Access as well as utilization of space now plays a vital role in Europe's social, economic, military and political power. The next years will only reinforce this trend thanks to major application programmes such as Galileo for navigation and localization and GMES for environment monitoring and for security.

The higher level of risks posed by the constant augmentation orbiting debris, heightened by recent orbital destructions operated by China and the United States, as well as more demanding satellite management procedures in an orbital context that will become more and more complex, both for public and private operators, are pleading in favour of a fully controlled European Space Situational Awareness (SSA) System.

In Europe, space object surveillance and space environment monitoring activities have been conducted for many years. The European Space Agency has been a prime contributor to the monitoring of the status of orbital debris and of the space environment for the safety of its own space missions as well as for the common interests of its Member States and of the international community. Other European member States have also developed technical facilities that are providing specific information about orbital objects, contributing to the setting up of a first cataloguing and knowledge base capability. Recent concept studies have already shown that a first operational SSA capability would be within the reach of Europe during the next decade.

This study is addressing both the governance and the data policy to be implemented for such a European SSA.

Four distinct services have been identified that would compose the SSA:

- Surveillance and monitoring of the space objects
- Imaging and characterizing the space objects
- Space weather forecast
- Near Earth-objects surveillance (NEO) tracking and monitoring

This mix of services and users obviously translates into a complex mix of regulations and responsibilities both from a public and from a private law standpoint. The diversity of user communities as well as the multinational aspects of SSA also require a very strictly structured data policy, especially as it may handle sensitive information at all levels of its utilisation, involving high-level political and operational responsibilities. Transiting from the existing national capabilities to a genuine European SSA system raises the issue of developing a common governance and data policy.

The final report is structured in three parts:

- A first part considers the generic requirements associated with SSA for each of the four services considered.
- A second part is devoted to the study of existing models of governance and data policy applied in various contexts (related to space applications or to domains

raising comparable issues). The goal is to highlight existing regulations and principles that can be usefully researched for SSA application.

- The final part of the study is intended to provide findings and recommendations for SSA governance and data policy. It proposes an initial governance and data policy model, stressing its relevance but also the critical issues to be addressed for further application.

2 – Organizing and summarizing the generic governance and data policy requirements for a European SSA

If a European SSA is naturally intended to ensure the most efficient protection system for any space asset as well as to protect as largely as possible from space-generated "accidents", a number of critical issues related to national and international security must be given consideration to help organize a sound governance and build a sustainable data policy. A clearly defined European SSA governance organization and data policy are essential to the development of a workable technical architecture.

The principal requirements for a European SSA system can be classified in four service categories mentioned above:

⇨ tracking and orbit determination of space objects;

⇨ imaging and identification of space objects;

⇨ space weather monitoring;

⇨ monitoring of Near Earth Objects;

The first two categories are concerned with man-made space objects, and could possibly be merged into one overall service category called "tracking and identifying space objects", while the other two services are concerned with the natural environment of planet Earth in the solar system.

Considering the four services envisioned, a European SSA governance and data policy will have to take into account the coexistence of different objectives and users. Three categories of users/ stakeholders are emerging in what remains in Europe a nascent activity (beyond normal national space objects monitoring):

⇨ The civil institutional users/stakeholders

⇨ The military users/stakeholders

⇨ The commercial users/stakeholders

Based on preliminary identification of needs by the SSA user group, several key requirements as collected via user groups meetings or expressed during more specific meetings can be synthesised as follows:

- The need for improved liability procedures in case of atmospheric re-entries or other launch or orbital events;

- A better regulation of orbital positions with a globally improved security procedure for collision avoidance in Low Earth Orbit (LEO);
- Improved information for operations linked to in-orbit relocation or to inclined orbit satellites;
- More relevant information based on a more reactive SSA system;
- Global picture of the space environment;
- Secured information and data management system, especially when handling security-sensitive data and information for business-related reasons.

Such key requirements have a direct impact on the general approach that can be adopted both for governance and data policy aspects. As far as governance is concerned, SSA functions present several specificities, involving the coexistence of public and private interests and associated responsibilities. It also implies the need to set up an organisation that can address both civilian and military issues, while satisfying the respective needs and practices of the associated user communities as described in the following scheme.

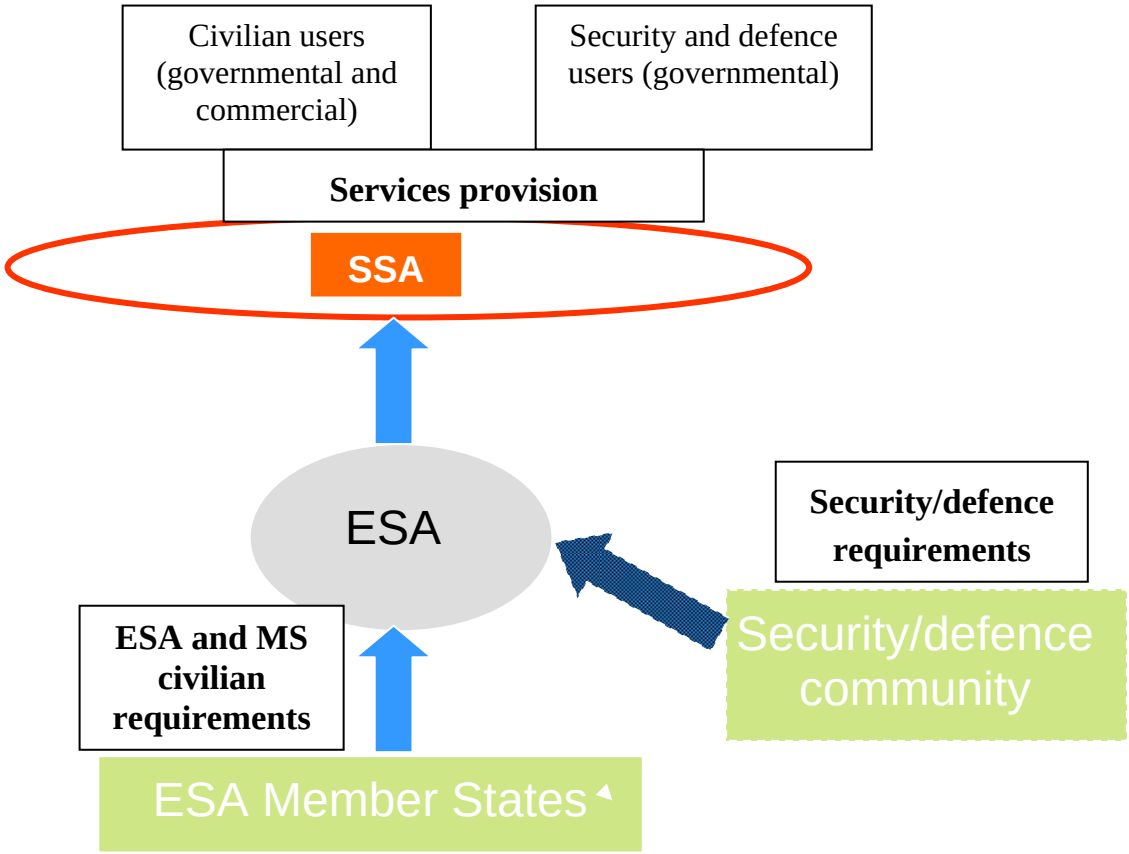


FIGURE 1: PRODUCTION OF USER REQUIREMENTS AND DEVELOPMENT SCHEME OF THE EUROPEAN SSA SYSTEM

This inherent SSA complexity makes the transitional mechanism between the experimental and the operational management periods particularly demanding. The actual operation of the different SSA services as well as their supervision will require some high level of attention by the public authorities, while preserving and even may be encouraging private service providers if and when possible for taking care of the operations and assuming associated responsibilities. The ultimate objective will be to favour a constant improvement of SSA services that will have to evolve according to technical improvements and feedbacks from experience.

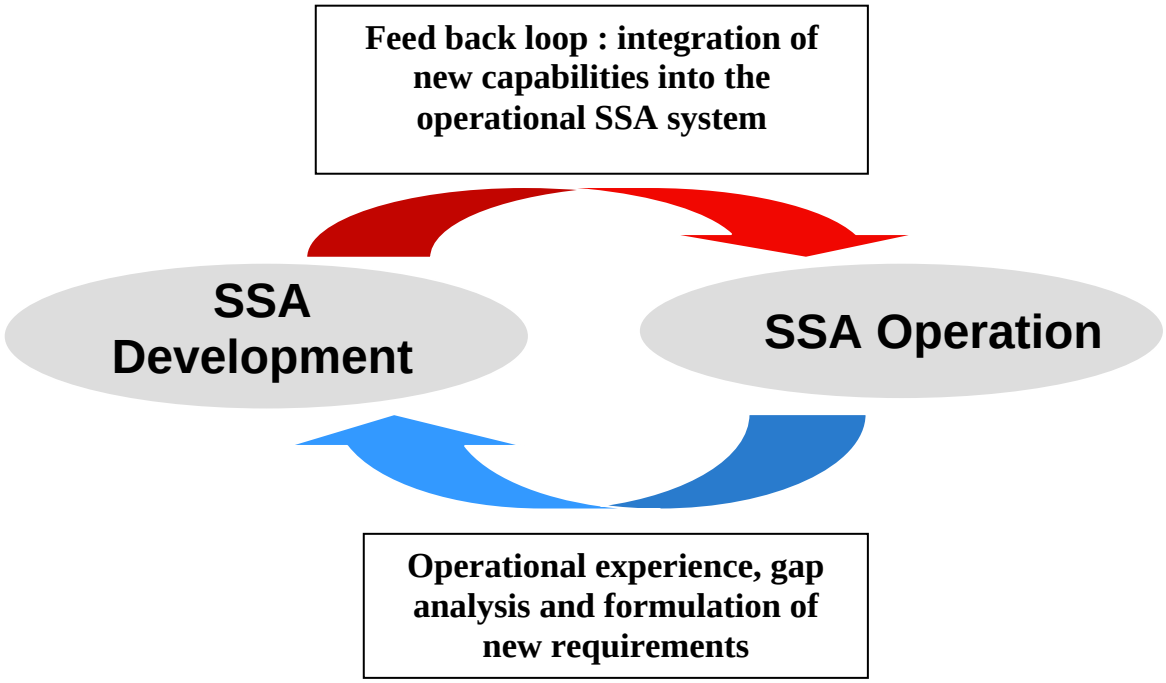


FIGURE 2: FEEDBACK MECHANISM FROM OPERATIONAL EXPERIENCE TO SYSTEM EVOLUTION

As far as data policy is concerned, and considering the key requirements mentioned above, a number of preliminary remarks can be made:

As mentioned in previous technical studies commissioned by ESA, a data itself is made of several dimensions that define its structure as shown on the following scheme:

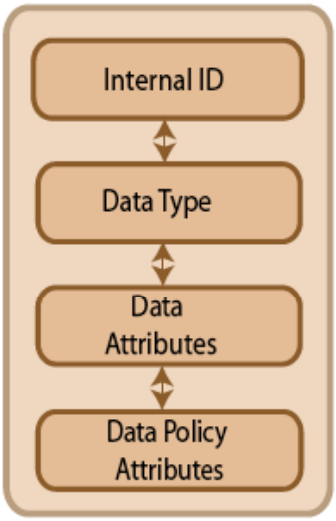


Fig. 3 : Proposed data structure

Such data cannot be considered alone and must obviously be associated to a given "service" as well as to its place in the SSA "chain of information". In order to set up an efficient data policy, the main steps of a complete sequence involving the data acquisition phase, the data processing phase, and the data dissemination phase must be considered.

When considering SSA data and information, three notions must be kept in mind in order to define the service provided by SSA and help understand how they can be organized in an efficient data policy framework:

- The existence of different SSA services
- Associated Data (as previously defined)
- Associated functions (acquisition, processing and dissemination)

A mix of the two first items of this list allows delineating the structure of the SSA generic requirements as shown in the following tables:

TABLE 1 – SURVEILLANCE AND MONITORING SERVICE RELATED DATA TYPES

Space object related data type	- Space object raw characteristics	- type - characteristics - date
	- Orbital characteristics	- Current orbital parameters - Current attitude - date
	- Space object related information	- Orbital history (recorded manoeuvres, related events, end of life) - Orbital predictability (collision analysis) - International designator - Launching country - Owner data - Operator data - Known functions - Service history (functional/non functional)
Request related data type	- Request history	- Request date - Request frequency
	- Request Type (requester information related)	- Defence related - General purpose related - Commercial user related
	- Request type (Nature of information)	- Raw data - Technical information - Contextual information
	- Request urgency	- Immediate priority request - Normal status - Special status (commercial service related)
	- Request status	- Incoming request - Request in progress - Satisfied request
Answer related data type	- Answer type	- Raw data type - High-level information type
	- Answer status	- Top Secret/Secret[1] - Confidential/restricted - Reserved (government/ commercial user related) - Open public access

[1] As referred in Doc ESA/C(2003)12, "*Security regulations Part 1: Basic Principles and Minimum Standards for the Protection of Classified Information Produced and Transmitted in Connection with ESA Activities*", 3 February 2003; and ESA/C(2003)95, "*Resolution on Security Regulations Part 2*", 25 June 2003.

TABLE 2 – SURVEILLANCE AND MONITORING SERVICE RELATED DATA ATTRIBUTES

Source	- Data tracability	- SSA sensors - Others
Destination	- Data tracability	- SSA Internal use - External use
Date and time	- Request related	- Originated request - Reception of Request - Processing steps
	- Data related	- Originated data - Processed data - Processed information
	- Answer related	- Originated answer - Transmitted SSA answer - External answer reception acknowledgment
Format	- Raw format (SSA/Non SSA sensor generated)	- SSA Internal use - External use (encryption/open)
	- Processed technical format	- SSA Internal use - External Use (encryption/open)
	- Contextual information (information message type)	- External use (encryption/open)
Quality	- Technical value degree	- SSA technical data - Non SSA technical data
	- Data integrity	- SSA controlled data - Mixed data - Uncontrolled (external) data

TABLE 3 – SURVEILLANCE AND MONITORING SERVICE RELATED DATA POLICY ATTRIBUTES

Confidentiality	- Top secret/ Secret/ Confidential/ Restricted	- Object related - Data type related - User related - International cooperation-level related
	- Proprietary Data	- Business confidential - Data type related - User related
	- Open distribution	- Open access - Data (Information) type related
Liability	- Government certification	- Government business certification
	- Legal certification	- Private business certification
Priority	- Immediate request - Urgent request - Non urgent request - Routine/Archive	
Information completeness	- Full completeness	- Technical data, meta data and information
	- Limited completeness	- Technical data and information
	- Very limited completeness	- Information
Data access type	- Unlimited registered user access	- Active encrypted full access (access: request from user to database)
	- Limited registered access	- Active encrypted limited access (access: request from user to database)
	- Restricted dissemination	- Active restricted dissemination (dissemination: no positive request – restricted internet access only)
	- Open dissemination	- Active dissemination (dissemination : no positive request – open internet access only)

TABLE 4 – SPACE IMAGERY SERVICE RELATED DATA TYPES (ADDITIONAL DATA TYPES)

Space Object related data type	- Space object characteristics	- Space object physical parameters (composition, form, length, estimated mass) - Space object features description (Sensor, Antenna, Energy source, attitude/ movements, sub-objects)
	- Space object environment characteristics	- Objects in vicinity
Request related data type	- Request type (Requester information related)	- Request origin
	- Request type (Nature of Information)	- Nature of the data/information requested - Level of imagery detail required
Answer related data type	- Answer type	- Raw data - Readable imagery - High-level information (imagery analysis)

TABLE 5 – SPACE WEATHER SERVICE RELATED DATA TYPES

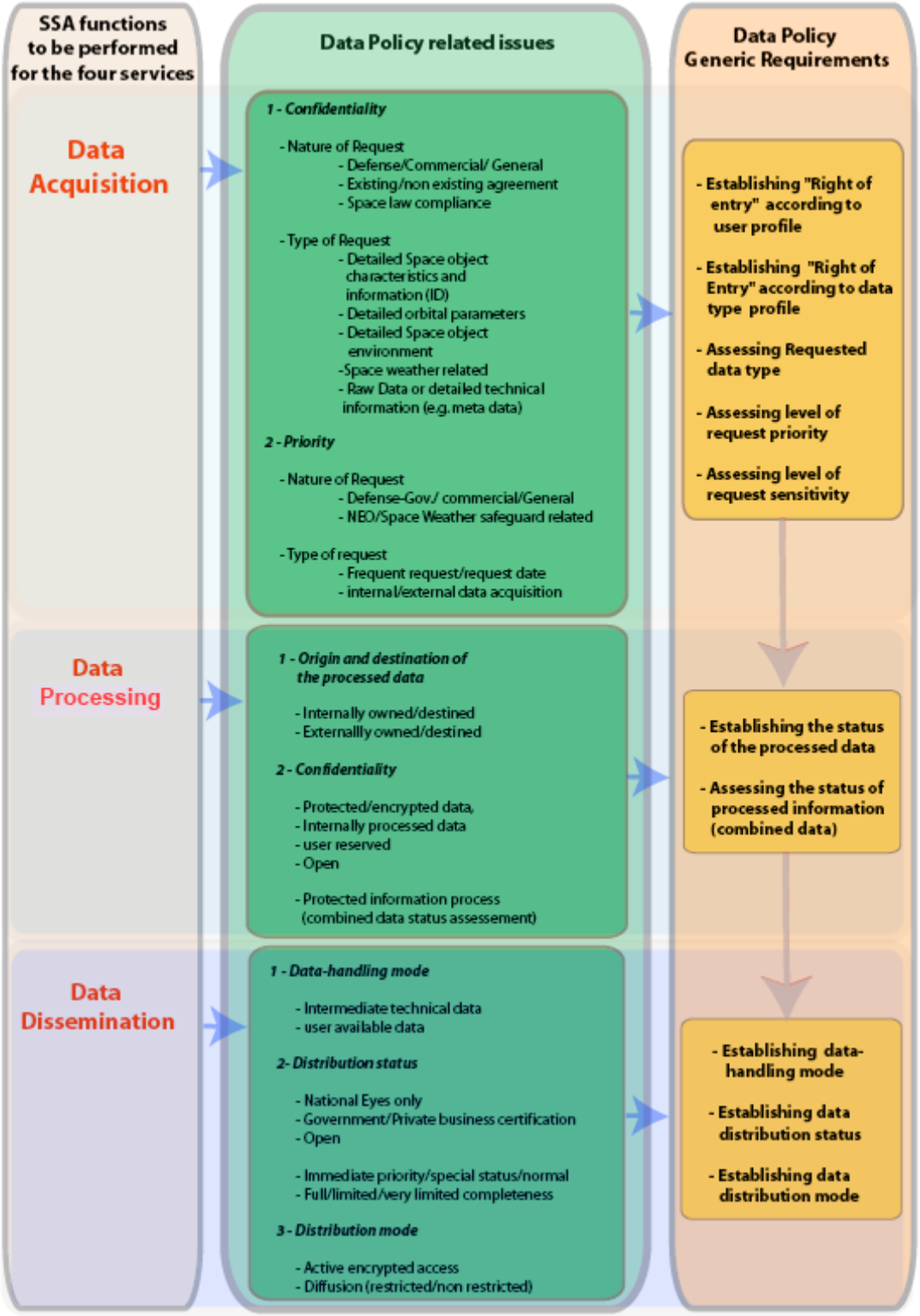
Space weather events/ phenomenon	Electronic fluxes	- Nature - Level - Origin
	Atmospheric density	- Level

TABLE 6 – NEO SERVICE RELATED DATA TYPES

Near Earth Objects	NEO trajectory NEO characteristics	- Origin - Sensor - Accuracy - Internal use - External use

In order to better understand how these initial requirements interface with the actual functions of a SSA system (i.e. data acquisition, processing and dissemination), a general summary scheme can be proposed to present a final list of generic SSA requirements:

Fig.4 : Summary of generic requirements as to Data Policy Rules linked to the structure of SSA system data



3 – Considering governance and data policy models for SSA

As a preliminary remark, and for the sake of accurate semantics, the term "governance" used in this study does not necessarily imply the existence of a concrete infrastructure (i.e. implying dedicated equipments and offices) but addresses only organisation and decision-making procedures in relation with the system ownership and operation management.

However, it is necessary to envision an innovative and dedicated organization to address the specificity of SSA in its operational phase. The efficiency of a European SSA will need a commitment from the Member States who express interest in improving space security. As such an interest is not uniform across Europe, this organization will necessarily reflect in its membership various degrees of implication by Member States. It is suggested that the Participating States to the initial SSA programme assess the respective merits of a new intergovernmental organization (similar to the EUMETSAT model) or a new ad-hoc dedicated agency of the European Union.

Several models can be considered that may provide a useful experience for handling sensitive information on a multinational basis. Some models can be found in the field of space applications or linked to the acquisition, processing and distribution of information produced by space systems. A range of applications is being considered covering a realistic range of programmatic and institutional specificities.

The following programs and structures have been analysed, for the following reasons:

1. GMES → "programme-oriented" infrastructure (mix of national existing and new European structures) and management;
2. Galileo → "programme-oriented" infrastructure based, at least initially, on a Public-Private Partnership (PPP) approach, supervisory authority, multi-level data;
3. TerraSAR-X → civilian programme involving a PPP-based approach;
4. Paradigm/Skynet V → military programme involving a PFI-based approach;
5. ORFEO → "Programme-oriented" bilateral inter-government agreement;
6. The European Union Satellite Centre (EUSC) → "Institution/policy-oriented" European Union integrated cooperation involving sensitive data policy;
7. EUMETSAT→ "Institution/Policy-oriented" multinational cooperation involving partially sensitive data policy
8. ESA → "institution/policy-oriented" Multi-national cooperation, non-sensitive data policy

A separate review has been conducted about possible governance and data policy models that have been implemented or designed in various domains that are not space-related but present relevant characteristics regarding the mix of the user communities and the level of sensitivity of the data and information exchanged. They are listed as follows:

- ⇨ the World Meteorological Organization
- ⇨ EUROCONTROL
- ⇨ The "Long Range Identification and Tracking" (LRIT) maritime surveillance system

Several analogies can be inferred from the analysis of these models for both governance and data policy related issues.

While the analysis of the legal aspects linked to existing "space" models shows that many solutions exist today that allow envisioning sharing duties and responsibilities for a future SSA System, it also shows the limit of the analogies with "Earth observation"-oriented activities.

- First of all, a SSA system does not survey nor focus on specific geographic areas on the earth surface, defined by their latitude and longitude, but address the whole outer space environment, which is not subject to national sovereignty.
- Second, in SSA, unlike in space based earth observation, there is no need to balance the interests of the sensed and sensing state. Quite simply, there is no "sensed state". However, when the space object under observation is another state satellite, certain rules as to distribution of information need to be considered.
- Neither UNGA Resolution 41/65 nor present laws and regulations relative to remote sensing of the earth apply to military satellite systems, while a SSA system encompasses a combination of military and civilian facilities.
- Furthermore, whereas in earth observation the sensing state provides its standard services to all states requesting it, SSA expressly foresees services on request, which may differ widely considering the types of data involved. Tracking a moving space object differs radically from imaging an area of the earth surface and will not induce the same type of support and technical activities.

For all the above reasons, the principles and existing regulations applicable to earth observation from space do not provide an adequate model for Space Surveillance Awareness.

With this limitation in mind, it remains that SSA can define a new model of cooperation and collective responsibility that may draw upon the experience gained by institutions such as EUMETSAT and the European Union Satellite Centre (EUSC). On the one hand, the EUMETSAT model is attractive because, similarly to what is expected for the European SSA, it developed as an ad hoc operational organization from an initial ESA experimental satellite programme. This approach has proven its validity over the years, to the satisfaction of its member states. Another option may be to consider a new independent agency of the European Union similar to such agency as the European Union Satellite Centre (EUSC), with technical facilities contributed by Member States

and by the European Space Agency itself (both ground based and space based facilities). The experience gained by the EUSC in the management and handling of sensitive information on a collective EU basis shows how such an organization can provide useful inputs regarding a future SSA governance and data policy. Nevertheless, such a model would also raise the issue of contribution by EU Member States who do not express interest for a European SSA, while some ESA Member States such as Norway and Switzerland may find it difficult to join an EU agency.

It results from the analysis of these existing models that no such models are fully compatible with the specificities of a European SSA. However, they all provide elements that allow envisioning the setting up an "ad hoc" intergovernmental SSA structure that can be both institutionally viable and fully operational while covering even the most sensitive aspects of SSA functions.

Examples drawn from the Air Traffic Control and even more from the new "Long Range Identification and Tracking" maritime surveillance system (LRIT to be put in place in 2008 at the international level) reinforce this case by providing the basis for what could be a relevant data policy structure for such an organization. The simple fact that data policy models can be implemented (as they have for many years in the field of Air Traffic Control) or are about to implemented (in the case of the LRIT) show how much robust data policy models can be designed for very demanding, real-time and highly protected information exchange between public users-military and civilian- and private operators.

4 – Findings and recommendations

4.1 – Preliminary remarks

Two categories of services must be considered separately in order to better identify specific critical issues. Some of these issues may be related to the entirety of the SSA functions, while others to only parts of the system.

When distinguished, the two categories of services (Surveillance, tracking and imaging services -i.e. space objects surveillance- and Space weather and NEOs services – i.e. space environment monitoring-) show clear differences implying both governance and data policy differences as inferred from figure 6 presented below.

- The first category presents the most challenging security and liability-related cases implying the identification of a number of specific issues to be addressed as a pre-requisite to any intra-European or international cooperation.
- The second category of services may be considered as easily manageable due to the relatively low security and liability-related constraints. In this latter case, the demanding constraints applied to the first category of services may not apply and less constraining management and practical organisations can be found to better optimise SSA services when possible

For these reasons, these cases are considered independently, with the objective of setting up governance and data policy procedures that can satisfy the requirements attached to the different services.

4.2 – A general scheme for SSA

A first general organisation can be presented that summarizes the structure of the European SSA organisation:

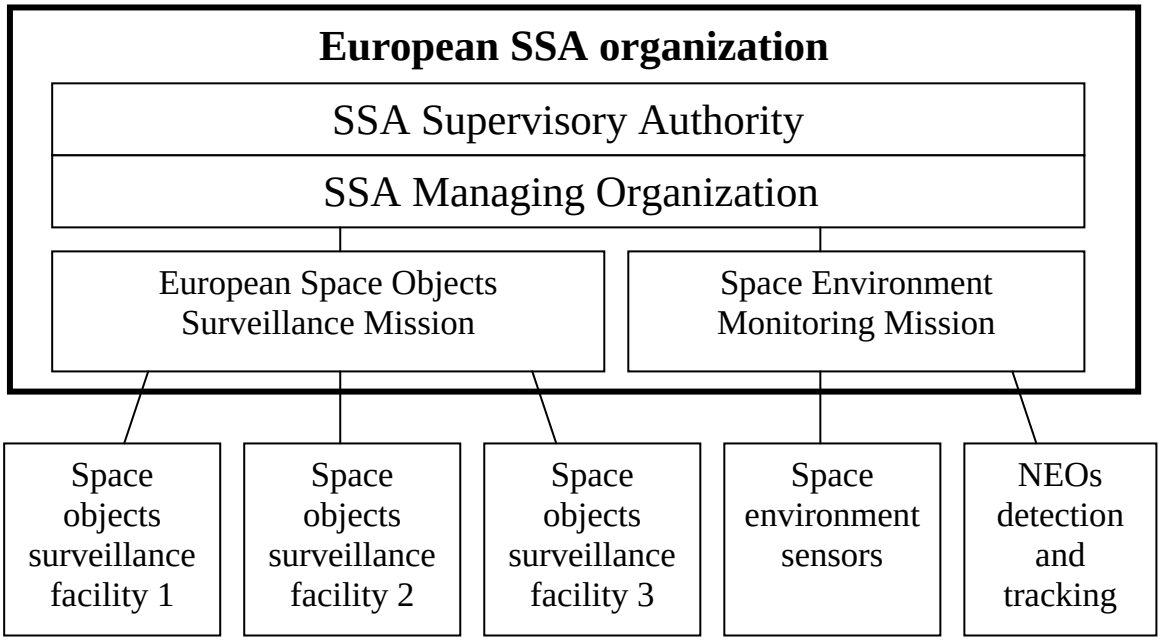


Fig.5-General outline of a possible European organization scheme for the European SSA

The organisation of the relationships of such a structure with both the European SSA "Contracting States" and the other actors located outside of the structure but possibly users and contributors to the system can also be represented in a functional scheme. For the sake of simplicity, three types of "outside" actors have then been considered; a European country having SSA tools at its disposal; commercial satellite operators and the general public.

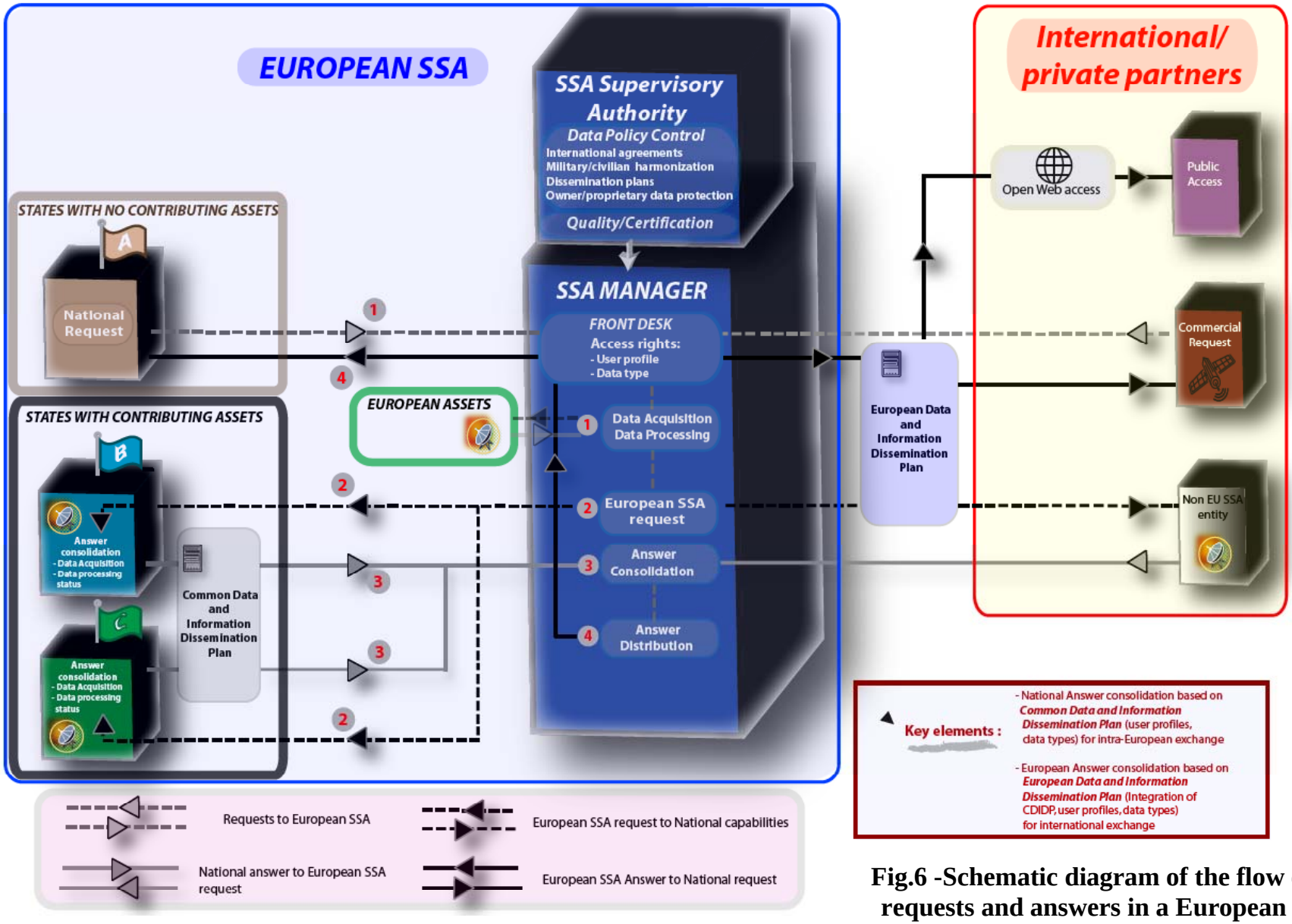


Fig.6 -Schematic diagram of the flow of information requests and answers in a European Space objects surveillance system

A number of critical issues must then be raised as they relate differently to space object surveillance and to space environment monitoring.

4.3 – Critical issues regarding governance aspects

4.3.1 – Space objects surveillance service

➡ ***<u>Regarding the governmental users and requests</u>: the governance structure must be capable of applying sufficient level of control as authorized by a commonly agreed supervisory authority.***

This implies :

- Military to Military arrangements:

The first critical issue which can be identified is the need for high-level intra-European military and security agreements accompanying the setting up of a European SSA system.

Taking into account the political sensitivity of the on-going construction process of a genuine European Security and Defence Policy (ESDP), besides an evolution of NATO structures, careful attention will have to be paid to the necessary consideration of the management of common military issues in the European SSA governance structure.

- Civilian/military arrangements:

In relation with the above remarks, the SSA governance should allow for the management separation of government users and commercial/other users. However, this separation does not have to impede the necessary technical and procedural coordination of a European SSA.

For this reason, a civilian-military coordination structure should be set up that allow managing priorities and other related issues in a real-time manner when necessary[2].

- International cooperation issues:

In order to increase its efficiency, any European SSA system will have to cooperate with non European government-owned SSA systems. All issues identified above apply to the management of international cooperation and the respective arrangements will have to incorporate specific rules specifically devoted to management of SSA international relations.

[2] The example of the Eurocontrol civilian-military commission can be quoted in this respect.

➡ ***<u>Regarding the commercial/other users and requests</u>: In this case, the governance structure must be capable to adapt its functioning to the commercial practices and rules in order to optimise the added-value brought to satellite operators in particular.***

Basically two options can be elected to produce the value-added services as expected by the users:

⇨ A first approach could consist in turning SSA products into public goods accessible to non-public users, each complying with security issues as evoked above.

⇨ Another approach could consist in allowing an authorised private service provider to sell adequate services to customers, leaving to this operator the charge to optimise the services according to the expectations of its customers. The interface between the SSA system and the private operator would be managed and controlled by the European supervisory structure.

With the double objective to keep the European SSA governance structure as easily manageable as possible and to promote SSA related economic activities, the second approach may be elected. In this case, the existence of a private service provider to exploit part of the SSA-produced information raises responsibility issues that have to be dealt with at governance level. Two main issues can be highlighted:

➢ Selection and licensing of a private service provider

Given the security considerations attached to SSA, any private service provider will have to be licensed and authorized by the SSA supervisory authority.

➢ SSA ownership and final service responsibility delineation

It appears that the extent of the system owner's legal responsibility in the commercial process leading to the service delivery to the final customer will have to be precisely delineated. More particularly, two issues must be addressed:

⇨ The careful definition of "system ownership"

⇨ The careful distinction will have to made between the "system functioning" guarantee and the quality of the service derived from this system in order to attribute clearly the legal responsibilities when service shortfall occurs.

Specific situations referring to security crisis or risks may be defined to justify the suspension or the end of the private service.

4.3.2 – Monitoring space weather and Near-Earth Objects services

These services do not imply as constraining governance procedures as for the space objects surveillance.

Considering the wide interest for such services, a particular attention will have to be devoted to rapid information-sharing mechanisms necessary to identify the source of disturbance. These mechanisms will have to be set up between the SSA state parties but also in relation with other international SSA systems.

Regarding the space weather related services, ESA should first identify the currently active operators, including the commercial service providers, analyse the current governance structure, taking into account in particular the new role that WMO is taking up in space environment/space weather monitoring, and the current information exchange mechanisms. It should then propose to its Member States appropriate governance and information-sharing mechanisms in accordance with security and confidentiality rules regarding the space objects and the users of the information. It is recommended that this particular activity be the subject of a "private service provider" approach

In the field of NEOs related services, the same process of identification and analysis of current governance and data exchange mechanisms should take place in order to avoid duplicating the existing governance structure, leading to appropriate governance within the European SSA.

4.4 – Critical issues regarding data policy aspects

4.4.1 – Critical data policy issues regarding the space objects surveillance

Considering the SSA model as proposed in this study, and consistently with the governance issues discussed above, the space object surveillance is setting the "reference" data policy to be further adapted to the second category of services.

➡ ***<u>Regarding the governmental users and requests</u>: the proposed data policy must be fully consistent with strong national and international constraints primarily based on security requirements.***

- Establishing user and request profiles

Refined user and requests profiles must established for authorized access to the system (triggering data acquisition procedures) considering the increased level of knowledge generated by an improved SSA system:

- Establishing "Data and information dissemination plans"

Considering the federative nature of the European SSA, so-called "Data and Information Dissemination Plans" (DIDP) must be considered as key elements of the

data policy. The role of such DIDPs in the SSA data policy is illustrated in figure.6. DIDPs will allow defining in advance and in a declarative fashion what information would not appear in the federated system for security reasons. The SSA system would justify the existence of two levels of DIDPs.

- First level: Establishing "Common Data and Information Dissemination Plans" (CDIDP) at national levels

CDIDPs would be based on governmental agreements between EU member states able to contribute to SSA and would provide the mean to federate intra-European capabilities by organising SSA data exchanges on the basis of national rules between the contracting States and the European SSA. CDIDPs would allow the "contracting governments" with contributing assets to restrict some information related to national security in response to certain requests from the European SSA system. CDIDPs would also impose constraints to the SSA system in all its components (national and European) when the information is requested from outside of the community of the SSA "contracting State (e.g. no "re-export" rule).

CDIDPs would be structured according to the request type (which space object requested?) and to the data type (what information request about a given space object?)

- Second level: Establishing a European Data and information dissemination plan (EDIDP)

The EDIDP would constitute the European security layer providing an interface between European SSA and third parties (non European government, commercial/other requester).

The EDIDP should assimilate CDIDP rules and as well as incorporate national regulations in European data acquisition and distribution practices in order to avoid unauthorized data/information re-export.

The EDIDP would also assimilate security policies of external partners to avoid re-export of unauthorized information, therefore taking into account security concerns expressed at the international level (extra-European data and information exchange).

➡ ***<u>Regarding the commercial/other users</u>: Commercial users such as geostationary satellite operators may be provided with the possibility to interact with SSA either directly or via a commercial service provider.***

Private operators should comply with the established EDIDP and use a single point of contact with European SSA.

Data produced by satellite operators would feed the European SSA in a confidential manner as their processing and re-distribution would go through the EDIDP with no re-export rule.

4.4.2 – Critical data policy issues regarding monitoring space weather and NEOs

As already mentioned, monitoring space weather and NEOs aims at the largest dissemination of information in real-time and do not appear as security sensitive as the space object surveillance.

Still, some confidentiality aspects may exist as for possible effects produced on satellites for example, leading to the production of possible government or proprietary business-related information.

As a consequence two types of information regarding space weather must be distinguished:

- ⇨ Space weather related data that should be the subject of the widest distribution
- ⇨ Effects-related information that should be the subject of restrictions when necessary

- ➡ ***Regarding the governmental users: Shared space weather service-related information regarding the effects produced on satellites may have security significance and would thus have to comply with the EDIDP for redistribution. Other NEO service related information would be shared with no EDIDP constraints.***

- ➡ ***Regarding the commercial/other users: Shared space weather service-related information regarding the effects produced on satellites may have commercial significance and would thus have to comply with the EDIDP for redistribution.***

- ➡ ***Regarding the international partners: Shared space weather service-related information regarding the effects produced on satellites of a non EU Government may have security significance and would thus have to comply with the EDIDP for redistribution. Other NEOs service related information would be shared with no EDIDP constraints.***

4.4.3 – Summarizing critical issues for SSA governance and data policy

For each considered services, the general organisation can include the most critical issues for SSA governance and data policy and then be completed as follows:

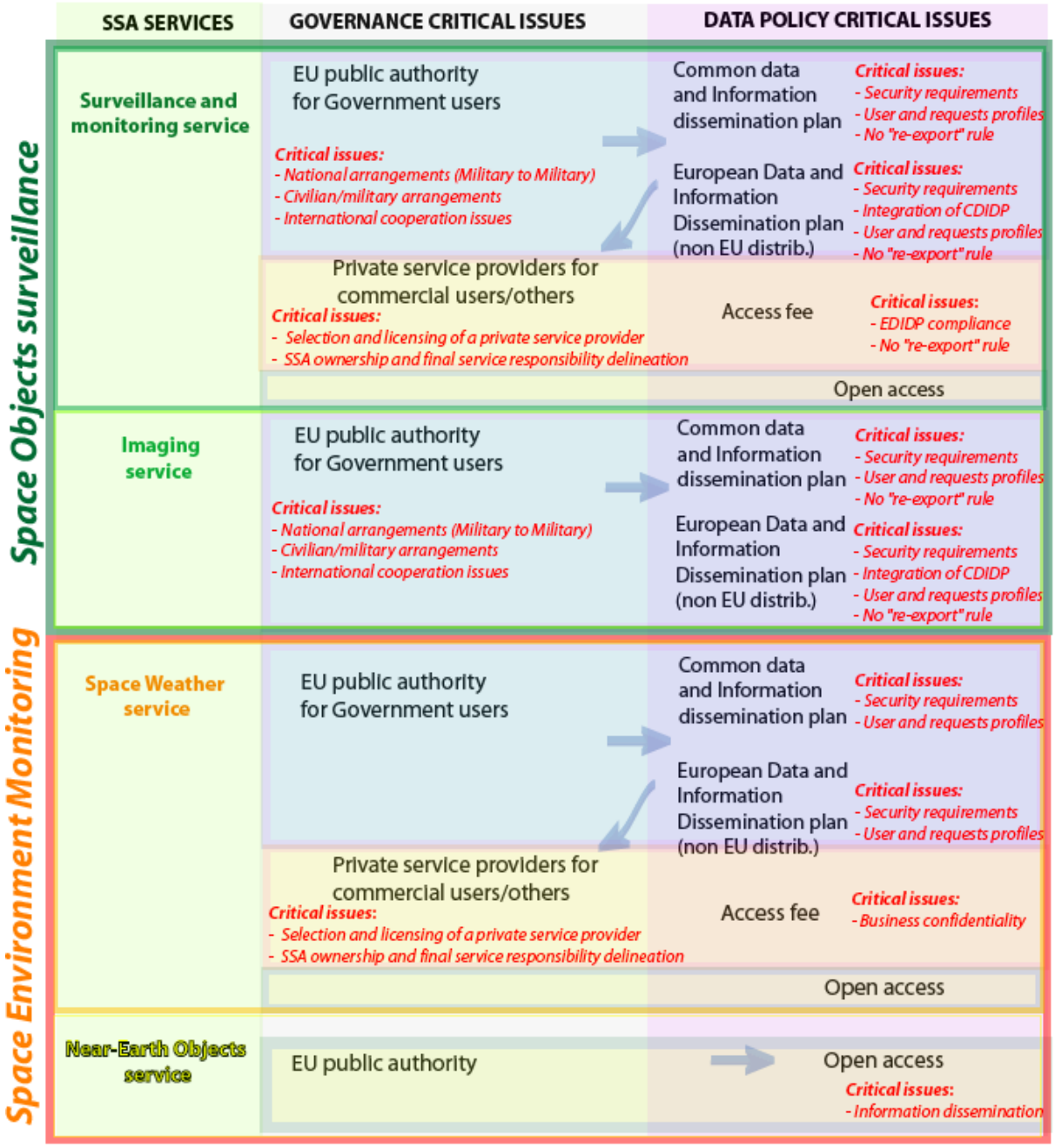


FIG.7: SSA GOVERNANCE AND DATA POLICY GENERAL ORGANISATION AND ASSOCIATED CRITICAL ISSUES

4.5 – Main findings

At least during an initial phase, any European SSA will consist in a federation of national and European technical facilities. This multinational nature affects strongly the applicable models for governance and data policy.

4.5.1 – European SSA governance

Based on this prerequisite and taking into account the identified generic requirements, the future SSA governance will be modelled around an intergovernmental structure[3] comprised of:

- a "Supervisory Authority" composed by so-called « contracting » states or governments (possibly at European Union level)
- a "managing organisation" which would play the role of harmoniser and federator of technical facilities that will be contributed by those contracting States putting their national public-owned capacities at SSA disposal
- a « civilian-military » exchange group on the model of Eurocontrol

A Board of Administrators composed of representatives of « contracting » governments, party states, possibly assuming responsibilities of launching or owning states, will guarantee the effective relationship between the national facilities and the SSA. They will also regulate any activity in SSA related to data acquisition, processing or dissemination.

Some resulting products would possibly be manageable by private operators for limited customer services provided by SSA.

4.5.2 – European SSA data policy

SSA data policy would be structured around two categories of services:

- Space objects surveillance (including surveillance, tracking and imagery services)
- Space environment monitoring (including space weather and Near-Earth Objects surveillance services)

- The first of these two categories is the most demanding service for both effective governance and secure data policy. The constraints are mainly oriented by the necessity to protect the access and the use of generated data. Two reasons are usually pointed at:
  - This service must ensure a complete protection of data related to sensitive space objects (mainly military but also commercial)

[3] The option of an "Ad-hoc" European Union independent agency inspired by examples such as EMSA, the EEA or the EUSC could present an alternative choice, with limitations related the specific perimeter of such agencies membership.

- This service must guarantee the protection of data related to the technical capabilities of contributing technical systems when those are military property.

➥ The « space environment service » is less demanding with a functioning based on strong interests and on a user community that is already structured. Some specific data would also be subject to protection given their possible sensitivity

The resulting data policy can be modelled following a previous experience set up by the International Maritime Organisation (IMO) in the field of maritime safety and security. Thus SSA data policy will be based on the following key concepts:

➥ "Common Data and Information Dissemination Plans" (CDIDP) agreed upon between SSA contracting Sates will allow establishing "access rights" to national facilities according to user profiles and data and request types (in line with the generic requirements). This allows the party State to protect sensitive data relative to a given space object or to critical events.

➥ A "European Data and Information Dissemination Plan" (EDIDP) will essentially play the same role for regulating the relationships between the European SSA and non-European users/requesters.

This two-stage data policy allows envisioning a baseline scheme that, according to this study, may answer the main demands for a fully effective and secure SSA while preserving possibilities for developing service activities managed by private operators if relevant from a business perspective.

♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦