Council of the European Union

Brussels, 22 March 2017
(OR. en)

7550/17

LIMITE

CSDP/PSDC 152
CFSP/PESC 274
COPS 103

COVER NOTE

From:	European External Action Service (EEAS)
date of receipt:	22 March 2017
To:	Political and Security Committee (PSC)
Subject:	High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM)

Delegations will find attached document EEAS(2017) 359.

Encl.: EEAS(2017) 359

EUROPEAN EXTERNAL ACTION SERVICE

Space Task Force

Working document of the European External Action Service

of 15/03/2017

EEAS Reference	**EEAS(2017) 359**
Distribution marking	***Limited***
To [and/or GSC distribution acronyms]	**Political and Security Committee (PSC)** **COSDP** **PESC** **COPS**
Title / Subject	**High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM)**

Delegations will find herewith the High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM).

On 12 December 2013[1], among the four programmes proposed by the European Defence Agency (EDA), the European Council welcomed the preparations for the next generation of Governmental Satellite Communication through close cooperation between the Member States, the Commission and the European Space Agency (ESA).

In 2016 the Global Strategy for the European Union's Foreign and Security Policy[2] identifies satellite communications as an area where investments are needed to ensure the Union's credibility and capability as a security actor.

The military user's requirements identified by the European Defence Agency in its Common Staff Target adopted in 2014 and the civilian user needs collected by the Commission have been merged to produce the High Level Civil Military User Needs for Governmental Satellite Communications. They have been presented to Member States experts both in the EDA project team and in the GOVSATCOM experts group established by the Commission.

Once endorsed by the PSC, the High Level Civil Military User Needs for Governmental Satellite Communications document will be used as an input for the impact assessment that could pave the way to a possible future initiative of the Commission. Such a new initiative will eventually be discussed in the Council and in the Parliament on the basis of a proposal by the Commission.

This document has identified the need to ensure the security of the communication for protecting EU Classified Information. However the way the future GOVSATCOM services should be accredited remains to be defined.

RECOMMENDATION

It is recommended that the PSC:

1. endorses the High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM) as a contribution to the Global Strategy for the European Union's Foreign and Security Policy;
2. suggests the Commission to liaise with National Security Authorities of the Member States, possibly in the Council Security Committee, in order to further explore the security implications of the high level user needs on the governance of EU GOVSATCOM services covering issues such as risk management and security accreditation.

Annex: High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM)

[1] Conclusions of the European Council – 19/20 December 203 – EUCO 217/13
[2] "Shared Vision, Common Action: a Stronger Europe", June 2016.

High Level

Civil Military User Needs for

GOVERNMENTAL SATELLITE COMMUNICATIONS

(GOVSATCOM)

TABLE OF CONTENTS

1 Introduction 5

1.1 SATCOM for Security and Defence 5

1.2 The evolution of SATCOM 5

1.3 Governmental usage of SATCOM and SATCOM Tiers 6

1.4 Towards an EU GOVSATCOM initiative 7

2 Scope and structure of the document 9

2.1 User needs and user requirements 9

2.2 Combining civil and military needs 9

2.3 Predicting the future 10

2.4 Structure of the Document 10

3 The EU GOVSATCOM initiative 11

3.1 Objective 11

3.2 Users of EU GOVSATCOM services 11

3.3 Specific use-cases 12

3.4 Main common operational needs 12

4 Risk acceptance for EU GOVSATCOM 13

4.1 Assured Access 13

4.2 Jamming and Interference 13

4.3 Interception and intrusion 13

4.4 Space operations 14

4.5 Cybersecurity risks 14

4.6 Geolocation of User Terminals 14

4.7 Dependence on third parties 14

5 Information Assurance Requirements for GOVSATCOM services 15

5.1 Security accreditation 15

5.2 Confidentiality, Integrity and non-repudiation of transmitted information 15

5.3 User Access 15

5.4 Control and Prioritization of GOVSATCOM services 15

5.5 GOVSATCOM "link status" service (LSS) 16

6 Common Needs 17

6.1 Interoperability and standards 17

6.2 Terminals needs 17
6.3 Frequency and Orbit allocation 17
6.4 Training and Concept of Use 18
7 GOVSATCOM Service for crisis management 19
7.1 Governmental users benefiting from the Service 19
7.2 Mission location, area and communication path 19
7.3 Supported communication services 20
7.4 Specific application to be supported 20
7.5 Time Constraints 21
7.6 Terminal needs 21
8 GOVSATCOM Services for surveillance 22
8.1 Governmental users benefiting from the Service 22
8.2 Mission area and communication path 22
8.3 Supported communication services, platform, terminal type 22
8.4 Mission Location 22
8.5 Time Constraints 23
8.6 Terminal needs 23
9 GOVSATCOM Services in support of key infrastructure management 24
9.1 Diplomatic Networks and Humanitarian Aid 24
9.2 Space infrastructures 25
9.3 Aviation 25
9.4 Land based transportation systems 26
10 GOVSATCOM services for specific use-cases 28
10.1 Specific user needs related to the Arctic Region 28
10.2 Remotely Piloted Aircraft Systems (RPAS) 28
10.3 Machine to Machine (M2M) and low data rate applications 29
11 Appendix 30
11.1 Definitions 30
11.2 Bibliography 30
11.3 List of abbreviations 32

Introduction

1.1 SATCOM for Security and Defence

Satellite communications (SATCOM) plays an indispensable role in security and defence related governmental communication. In particular, they are used when other, ground-based, means of communication are not possible, reliable, or available. For a range of governmental tasks and services in the EU satellite communication is an essential tool, especially in crisis situations or other cases related to the security and defence of citizens.

Satellite Communications complement terrestrial communication networks, which they seamlessly link and extend.

1.2 The evolution of SATCOM

Originally designed for military purposes in the sixties, SATCOM services have quickly evolved to meet civilian communication needs: intercontinental and regional communication from the seventies to the eighties, TV broadcast since the nineties, and more recently multimedia applications.

Nowadays, most of the world's satellite communication capabilities are used for TV Broadcast (see BSS below) and general public multimedia applications. Global and maritime mobile communications services have also evolved into a variety of applications with the development of hand held and mobile satellite terminals which are now available for the general public.

Satellite communication services and applications form the largest space market sector and are sold on a "global open market". SATCOM "capacity" is usually delivered by satellite operators who own a fleet of satellites which they procure, launch, and operate.

The increased information demand of decision makers, coupled with new technologies from the Internet and significantly improved sensors, will lead to a growing demand for SATCOM services over the next decades.

With the "new Space" and in particular the entry of new business actors from the "digital economy" the SATCOM market could face considerable changes and may lead to new or modified business models, SATCOM services and frequency allocations.

It has been agreed worldwide to allocate specific frequency bands to specific SATCOM services. The use of the radio-frequency spectrum and the geostationary-satellite and non-geostationary-satellite orbits is governed by the international 'Radio regulations' (RR) treaty.

At international level the International Telecommunications Union, as specialised agency of the United Nations, manages the negotiations and revisions of the RR Treaty, in particular through the World Radio Conferences (WRC) which is held every four years.

At national and regional level the allocation of frequencies and orbits to services is managed by the competent national authorities.

The RR [1] distinguishes the following SATCOM services:

- fixed-satellite service (FSS)
- inter-satellite service (ISS)

- mobile-satellite service including (MSS)
    - land mobile-satellite service
    - maritime mobile-satellite service
    - aeronautical mobile-satellite service
- broadcasting-satellite service (BSS)

With the variety of satellite frequency bands that can be used for SATCOM, designations have been developed so that they can be referred to easily. Traditionally the C (4-8GHz), KU (12-19 GHz) and Ka (26-40 GHz) band are allocated to the fixed satellite services and the L band (1-2 GHz) to mobile satellite communication.

In addition the RR defines a space operation service concerned exclusively with the operation of spacecraft

Traditionally, the FSS and MSS sectors operated in different markets and provided fundamentally different services to different customers. One of the major industry trends of the past few years has been the gradual blurring of the lines between MSS and FSS.

Finally, some SATCOM frequency bands (X-band: 8-12GHz, and part of the Ka-band) are dedicated to governmental use.

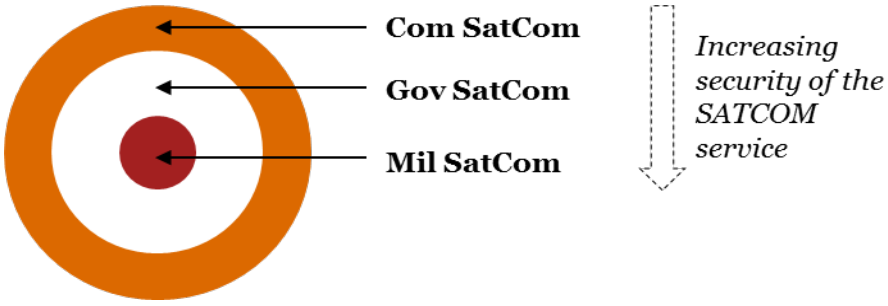
Frequency regulations constraints and orbital reservation are very significant points to be tackled early in any SATCOM project (see 6.3).

Governmental usage of SATCOM and SATCOM Tiers

Public authorities, and in particular the military forces, have had recourse to SATCOM derived from both publicly owned satellite and services procured on the market.[3]

There is a general understanding that the provision of Satellite Communications services (SATCOM) for governmental use can be divided in three tiers which corresponds to different levels of information assurance although the exact definition of each tier may slightly vary.

The following descriptions of the three tiers are based on the Common Staff Target GOVSATCOM (2014) from the European Defence Agency.



1 MILSATCOM: MILSATCOM is highly protected and guaranteed SATCOM, generally provided by military systems, offering highly assured and protected satellite communication capacity both in terms of nuclear hardening, anti-jamming/dazzle

[3] The US Defense Information Systems Agency (DISA) is the biggest Governmental source of COMSATCOM procurement but it is US intention to mitigate DOD's future reliance on commercial SATCOM. [21]

capacity and highly secure telemetry, tracking, and command (TT&C), supplemented by an equally robust and resilient ground segment. The security and technology are highly specific and largely sovereign in nature. Those MILSATCOM systems are primarily designed for military purposes and are under national control.

2 GOVSATCOM: GOVSATCOM are "highly assured SATCOM offering a certain robust security level with some resilience …. GOVSATCOM systems are generally referred to as less protected than MILSATCOM systems."

3 COMSATCOM: Service/Commodity based procured satellite communication capacity on the global open market providing a degree of 'on-demand' access.

Towards an EU GOVSATCOM initiative

The relevance, importance, and timeliness of an EU GOVSATCOM initiative are widely shared by EU nations in the Council and by the European Parliament.

The 2013 European Council in its conclusions [2] *"remains committed to delivering key capabilities and addressing critical shortfalls through concrete projects by Member States, supported by the European Defence Agency"*, it welcomes*" in the area of "Satellite Communication: preparations for the next generation of Governmental Satellite Communication (GOVSATCOM) through close cooperation between the Member States, the Commission and the European Space Agency."*

As a preliminary step for a future GOVSATCOM initiative the December 2014 Competitiveness/Space Council in its conclusions [3] *"welcomes the initiatives to identify user requirements regarding GOVSATCOMs by the Commission on Civilian User needs and EDA on military user needs" and "UNDERLINES the need to avoid fragmentation of demand and to foster civil-military synergies for the preparation of the next generation of Governmental Satellite Communication through close cooperation among Member States, EDA, the Commission and ESA"*

The European Commission in its 2016 work programme [4] has approved an initiative on Defence with a roadmap on an action plan proposing to *" Provide greater support for national and European space capacities and capabilities, in particular in the area of Government Satellite Communications (GOVSATCOM), secured communications through satellites used by public authorities, which would reinforce synergies between space related activities and defence." GOVSATCOM is also referred to in the Roadmap of the Space Strategy adopted in October 2016.*

In November 2014, the steering Board of the European Defence Agency in ministers of Defence formation endorsed a high level military needs document on GOVSATCOM named Common Staff Target [5] and EDA subsequently launched a feasibility study in June 2015 to further analyse defence GOVSATCOM requirements.

In June 2016 the European Parliament adopted a report titled "Space capabilities for European security and defence [6] in which it "*Welcomes the work being done to provide the EU with autonomous access to governmental satellite communications (GOVSATCOM) and invites the Commission to continue to make progress on this file; recalls that the first step in the process was the identification of civil and military needs by the Commission and the European Defence Agency, respectively, and considers that the initiative should entail the pooling of demand and should be designed in a way that best meets the needs identified;*"

GOVSATCOM has been identified a one of the element of the Global Strategy [7] and of the implementation plan on Security and Defence [8].it will contribute to EU response to Hybrid Threats [9], it can also support EU maritime strategy [10], and to the Arctic Policy [11].

The GOVSATCOM initiative is part of the Space Strategy for Europe [12] and the European Defence Action Plan [13].

Finally, this initiative is referred to in the letter of intent accompanying the State of the Union 2016 by President Juncker [14].

Scope and structure of the document

The purpose of this document is to contribute to the development of an EU GOVSATCOM service in line with the civilian and military user needs in the EU.

For the time being, civilian governmental users are mainly procuring COMSATCOM services. But some specific needs of governmental users, especially in relation to security, lead to requirements which are either incompatible with requirements of the majority of COMSATCOM customers, or would only be procured by governmental actors on the global open market at a high price. The EU member States and the European Parliament have expressed the need to develop a new type of European level SATCOM service dedicated to civil and military governmental and EU institutional needs. Such a GOVSATCOM service should complement the currently existing COMSATCOM and MILSATCOM services.

In the defence domain, GOVSATCOM shall provide assured access to SATCOM resources to satisfy Information Exchange Requirements (IER) for actors involved in the conduct of CSDP operations derived from the EU Level of Ambition [7] and provide capacity to support each Member State specific IER. GOVSATCOM capability will be an essential component for maintaining command and control and delivering both information superiority and operational autonomy to EU operations in order to achieve tactical and operational objectives.

User needs and user requirements

This document is a high level user need document. It aims at proposing a set of general principles applicable to all EU GOVSATCOM services and at identifying major trends regarding user needs. Contrary to a user requirement document, it does not aim at describing the detailed specification of given GOVSATCOM services for specific user communities, at quantifying user needs, nor at proposing technical architecture solutions. These aspects will be studied at a later stage of the process by different actors depending on the solutions which will be retained for the provision of GOVSATCOM services.

Combining civil and military needs

This document is the synthesis of two high level user needs documents:

1. The military user needs document produced by EU Member States military experts within the Project Team SATCOM of the European Defence Agency. This document entitled Common Staff Target for Governmental Satellite Communications has been endorsed in November 2014 by the Steering Board of the EDA
2. The high level civilian user needs documents has been prepared by a Commission expert group composed of EU Member States experts in Governmental Satellite Communications. It has been presented to the Council Space Working Party on the 18 October 2016.

In line with the European Council conclusions to foster synergies between civil and military needs this joint civil military user needs documents has been prepared by a GOVSATCOM coordination group consisting of representatives of the EC, EDA, ESA and the EEAS.

This document identifies the high level needs of governmental civilian and military communities of SATCOM users, and provides first guidance for governmental satellite communications (GOVSATCOM) service.

Some of the missions, operations and use-cases described may be performed by civilian or military entities. The needs expressed in those cases are therefore by default common to civil and military users

The detailed conditions and the governance structure under which the GOVSATCOM service will be made available to the users is not described in this document.

Predicting the future

The difficulty when proposing a user needs document in the area of communication and information systems is to anticipate technology evolutions which may revolutionize user practices and therefore completely change the user requirements. The changes induced by the various "internet revolutions" illustrate this impossibility to fully anticipate user uptake of technology.

This high level user needs document aims at agreeing among the various governmental user communities' principles and needs which could be valid regardless of the technological trends affecting communication practices. In parallel the document will highlight some technology trends which could rapidly evolve the user requirements.

This document may need to be regularly updated as both technology and user practices evolve.

Structure of the Document

The document is structured as follows:

- Chapter 3 sets the perimeter of the high level user needs in terms of targeted user communities and overall operational needs.
- Chapters 4, 5 and 6 describe the general logic in developing the high level user needs for EU GOVSATCOM services, addressing general principles regarding the acceptable level of risks for the users of GOVSATCOM services, general principles regarding information assurance and general considerations and constraints which apply to all GOVSATCOM services.
- Chapters 7, 8 and 9 describe specific families of GOVSATCOM user scenario's which correspond to similar types of SATCOM usage and risks.
- Finally chapter 10 highlights use-cases that deserve specific attention since they correspond to a rapid and potentially disruptive evolution of user needs pushed by new communications practices, or could be insufficiently covered by existing systems.

The EU GOVSATCOM initiative

Objective

The general policy objective of an EU GOVSATCOM initiative is to ensure reliable, secured and cost-effective satellite communications services for EU and national public authorities managing security critical missions and infrastructures.
Specific objectives are:

To overcome the fragmentation of SATCOM governmental users on European scale, seeking synergies between the civil and military domains.

To find solutions which ensure an appropriate guarantee of access for governmental users (EU and national) to satellite communications.

To ensure that solutions are sufficiently robust to ill-intentioned acts to be used by EU governmental security and defence actors.

To ensure that the solutions provide an appropriate level of European non-dependence in terms of technologies, assets, operations and services. This requires a competitive and innovative European space sector to ensure renewal of systems in the mid-2020's. [15]

Users of EU GOVSATCOM services

The following civil and military GOVSATCOM user communities have been identified, at European and national level.

- Military Forces of the EU Member States (involved in national, EU or coalition operations)
- Border surveillance authorities
- Maritime community
- Police forces
- Civil protection
- Humanitarian aid
- EU external action (including actors involved in the conduct of CSDP missions and operations)
- Civil and Military operators of key infrastructures - sometimes related to the above listed user communities – benefitting from EU GOVSATCOM services such as :
    - Institutional and diplomatic networks of the EU and Member States
    - Transport infrastructures: e.g. air, rail and road traffic management
    - Space infrastructures & services including EGNSS (EGNOS and Galileo) and Copernicus

Specific use-cases

The following use-cases deserve specific attention because of on-going political discussions and technological trends:

- User communities in the Arctic region have a growing need for GOVSATCOM which is not met by the current European communication systems (see 10.1)
- There is a need for a GOVSATCOM service which will enable a growing use of Remotely Piloted Aircraft System (RPAS) for Beyond Line of Sight (BLoS) Communications (see 10.2)
- Low data rate secured communication (see 10.3)

Main common operational needs

The GOVSATCOM service shall provide assured and secured access to SATCOM resources to satisfy information exchange needs of governmental or governmentally authorised users.

Common operational needs for GOVSATCOM services[4] include:

- Possibility to relay any type of information content (voice and audio, any type of data file, video, images) both through messaging and real time streaming applications;
- Web connectivity (possibly through IP services) but also short digital messages relay (SMS type);
- flexibility and scalability of service upon demand;
- geographical coverage appropriate to the specific GOVSATCOM needs described in chapters 7 to 10;
- integration into fixed and mobile platforms.

[4] Some of these requirements could be specifically addressed through different dedicated GOVSATCOM services but the portfolio of EU GOVSATCOM services shall cover all the above needs.

Risk acceptance for EU GOVSATCOM

All SATCOM services offer the same type of services to the users (c.f. 1.1). The main difference between the MILSATCOM, GOVSATCOM and COMSATCOM services is the level of risks that the users are ready to accept whilst making use of the service. The aim of this chapter is to describe in general terms the risk acceptance for the users of EU GOVSATCOM services.

Assured Access

The EU GOVSATCOM users need the assurance that GOVSATCOM service or resources are guaranteed and cannot be pre-empted by non-governmental users or third parties. (The prioritisation of the GOVSATCOM services among the Governmental and Institutional users is addressed in 5.4.)

GOVSATCOM users need a link recovery function to restore any broken communication with a maximum delay time to be defined with the user communities.

Jamming and Interference

GOVSATCOM services must be resilient to interferences and should offer technical and procedural means to quickly remedy any interference occurring on a GOVSATCOM service.

GOVSATCOM operators should be capable to providing relevant governmental authorities, corresponding to the various users of the GOVSATCOM services, with relevant information on the location and type of interference/jamming source to allow for appropriate response.

In view of defining the next generation of GOVSATCOM services, a risk assessment of the threat environment related to jamming and interference must be conducted to precise the level of threat and develop a corresponding range of GOVSATCOM services.

Next generation GOVSATCOM services shall offer anti-jamming capabilities commensurate with the risk to which civilian governmental users are exposed. In particular some GOVSATCOM users could operate in the presence of "improvised" man-made jammers. However GOVSATCOM services shall not offer the "MILSATCOM type" of anti-jamming capabilities that are designed to resist advanced military satellite jamming techniques.

Interception and intrusion

GOVSATCOM services should allow guaranteed protection against any attempt to intrude connected information systems or to intercept transmitted data and information.

This risk should be assessed at any stage of the process leading to the delivery of the GOVSATCOM services: including the ground and space segments, at the level of the deployed technologies, the industrial processes, the launch and operations of the satellites, and the users. (See also section 6.)

Satellites and payload hosting GOVSATCOM services shall be protected against any attempt to break into satellite and payload control systems including at the level of the Command and Control (C2) Links of the satellite, the on-board processors and the ground control and mission segments.

Space operations

Operators of satellites providing GOVSATCOM services shall mitigate risks related to any natural threat in orbit, such as space debris and space weather phenomena, using state of the art information services. In this respect the services developed in the framework of Decision No 541/2014/UE for Space Surveillance and Tracking (SST) will offer a level of European Autonomy which should be used to support space operations.

Operators of satellites providing GOVSATCOM services shall respect the applicable laws and regulations on space operations including for the launch of the satellites.

Cybersecurity risks

In line with the principle set by Cyber Strategy of the European Union [16] and by the NIS Directive [17], specific attention needs to be paid to cybersecurity risks to ensure that

- GOVSATCOM services delivery is ensured
- GOVSATCOM communication links are not an entry point for cyberattacks on users Information systems.

Effective and proven countermeasures shall be implemented both at the level of the space and ground (control and user) segments.

Geolocation of User Terminals

The GOVSATCOM services should seek to protect the location of the user terminals. In particular the operator of GOVSATCOM services should protect as required any information which could lead to an unintended disclosure of specific user's location.

Dependence on third parties

As part of the above needs, specific attention shall be paid to the possible risk of dependence on third parties (Third States and/or non EU Organizations) which could hamper the autonomy of action of the EU and its Member States.

GOVSATCOM services shall be subject to a specific analysis to assess possible dependences to thirds parties and their consequences covering each element involved in the GOVSATCOM provision including (the list is not exhaustive):

- Both space and ground technologies at components, subsystems and systems level.
- Manufacturing industries (through the entire industrial lifecycle with a specific attention to the jurisdictions and to the shareholders composition)
- Owner and operators of the space systems (including personnel, shareholders, satellite launch, registration and licensing States and/or Organizations)
- Physical location of the various components of the GOVSATCOM systems (ground control, monitoring, TT&C systems)
- Accreditation and Certification bodies

Information Assurance Requirements for GOVSATCOM services

GOVSATCOM services need to be capable of transmitting EU Classified Information (EUCI) up to "EU Secret" level and the equivalent level of national classification in all EU Member States. GOVSATCOM services need to follow the principles set in Council Decision of 23 September 2013 on the security rules for protecting EUCI [18] and the specific needs listed below.

Security accreditation

Systems and organization delivering GOVSATCOM services shall be subject to a risk assessment validated by a security accreditation body, recognised by the EU. This body will assess all security aspects, including technology, industrial processes, launch and operations, ground and space segment and terminals, personnel and infrastructures.

GOVSATCOM services require levels of security accreditation which should be guaranteed by one or several National Security Agencies of EU member States and should be commensurate with the level of risk associated with the GOVSATCOM service considered.

Confidentiality, Integrity and non-repudiation of transmitted information

GOVSATCOM services shall ensure confidentiality, integrity and non-repudiation of the information transmitted either by ensuring

- compatibility with end to end cryptographic solution
- encryption of the channelled information as part of the GOVSATCOM service.

The governmental crypto equipment used has to be commensurate with the criticality of the mission, the nature of transmitted information and the level of threat.

User Access

GOVSATCOM Services shall allow tailored user access which should be managed at central and also at local level and by each user community and offer a level of protection against intrusion and compromising, commensurate with the criticality of the mission, the information transmitted and the level of threat.

Control and Prioritization of GOVSATCOM services

GOVSATCOM shall ensure a flexible and efficient management of the GOVSATCOM services according to the following principles:

- Both the EU and the individual Member States need to have assured access to their agreed share of the GOVSATCOM resource and have the possibility to internally prioritize users.
- Each user community needs the flexibility to manage the GOVSATCOM services according to their specific needs.
- Local users of the same GOVSATCOM service shall have the possibility to manage the resources locally.

GOVSATCOM "link status" service (LSS)

User of the GOVSATCOM service shall monitor the risks associated with the service both during the planning and conduct of the various missions and operations.

The delivery of GOVSATCOM services shall be coupled with a "link status" service (LSS) informing the corresponding users on the status of their GOVSATCOM services and monitoring assessing and forecasting the associated risks described in chapter 4.

The level of information provided shall depend on the type of GOVSATCOM service and on the final user. While the information displayed on a user terminal could only inform on the availability of the link, the LSS could provide more detailed information to assist operation managers in planning, securing and operating multiple information systems.

Common Needs

Interoperability and standards

GOVSATCOM services need to comply with the relevant standards of relevant user communities, both for satellite communication and related to interoperability with existing ground infrastructure.

New GOVSATCOM services need to evolve towards the use of open standards. The general principle is to promote the development of future GOVSATCOM terminals through the adoption of open and standardized waveforms.

In some cases a hand-over capability may be needed. This is the capacity for a device to seamlessly switch from terrestrial communication system to a satellite one and vice versa. Such a hand-over capability would also need to be standardised.

Terminals needs

GOVSATCOM users should master the choice and the acquisition of the GOVSATCOM terminals.

Deployment, operation and maintenance of GOVSATCOM terminals are essential elements of the GOVSATCOM Services.

GOVSATCOM services should allow depending on the circumstances:

- the use of legacy terminal equipment
- the local purchase of user terminals with little modification to allow the delivery of GOVSATCOM service.
- for other services the provision of GOVSATCOM terminal equipment can be an integral part of the GOVSATCOM services.

Any GOVSATCOM user terminal shall undergo a specific functional compatibility and security accreditation process (see 5.1) to ensure that the usage of the terminal does not pose risks to the GOVSATCOM systems, services and users.

Frequency and Orbit allocation

Provided that the continuity of the GOVSATCOM services shall be ensured, the EU and the Member States which are involved directly or via (a) satellite operator(s) which is(are) operating on their behalf or under their jurisdiction, shall take the necessary measures both at national, European and international level to protect and secure the frequencies and orbital positions that are allocated for (or involved in) the provision of GOVSATCOM services, including for the future generation of EU GOVSATCOM services both at national European but also international level including ITU.

Training and Concept of Use

Training will be needed to ensure the appropriate qualification of both civil and military staff involved in managing, operating or using (if applicable) GOVSATCOM in accordance with their area of responsibility. Therefore, GOVSATCOM resources shall be made available as appropriate where those assets are stationed.

GOVSATCOM Service for crisis management

GOVSATCOM shall allow the provision for assured high data rate satellite communications over crisis areas in a scalable manner.

In particular GOVSATCOM capability must be able to provide sufficient guaranteed capability for initial deployment and should be able to scale up in a timely manner if additional capacity is required.

GOVSATCOM crisis management services should also be made available for exercises and training of the various security and defence forces listed in 7.1.

Governmental users benefiting from the Service

This service should be made available to:

- Military forces of EU Member States
- Civil Protection workers,
- Police and Homeland Security Forces
- CSDP missions and operations
- Humanitarian aid responders, including NGO operating on behalf of the EU or Member States
- Local EU and National delegation concerned with the crisis (see 9.1)
- Other governmental actors involved in Crisis Management activities

Mission location, area and communication path

Although crisis management mission and operations are likely to take place anywhere in the world it is considered that the most stringent needs are in continental Europe and its neighbouring regions (Africa, Mediterranean, Middle East Asia, Arctic, Atlantic).

EU GOVSATCOM needs to be able to support up to **fifteen simultaneous crisis management operational zones**.

Should a crisis management operation take place in the Arctic area, particular needs may apply as described in 10.1

GOVSATCOM solutions also need to cover overseas territories under the control of an EU Member State.

First responders shall benefit from GOVSATCOM communication services in an area of around **1000 km in diameter over the crisis area**.

Each GOVSATCOM user in the mission area shall have access to

- Other GOVSATCOM users within the same mission area,
- Reach back capabilities to its rear bases and coordination centres, usually in EU Member States, including supported network infrastructures communication and information system, and including NATO facilities (ACO) in case of activation of the Berlin+ Arrangement.

- Local Networks deployed by the user including supported network infrastructures communication and information system.
- Public communication networks (e.g. Internet, PSTN).

Supported communication services

The following types of satellite communication services need to be supported

- Short Video on the move
- Video conferencing (fixed)
- High data rate VSAT Communication (Fixed and on the move)
- Voice (fixed and on the move)
- Images (fixed and on the move, high and low resolution)
- Broadcast and Multicast data services (fixed and on the move)
- Low to medium data rate systems (fixed and on the move)[5]
- IP services such as Email, messaging, chat
- Remote and secured access to specific information systems

Specific application to be supported

GOVSATCOM crisis management service should be used to support the backbone communication infrastructure between the various command and control centres (in the military between the strategic operational and tactical kevels including OHQ and FHQ) and for civilian responders between the rear bases and the deployed command posts.

In addition the GOVSATCOM crisis management service shall support the following type of applications:

- ***Telemedicine:*** GOVSATCOM Crisis Management service shall support health care services, such as access to specialists, to the remotest of areas where teams are deployed. With increasing medical capability that relies on ICT (Information Communication and Technology), such as X-Ray, CT (Computerised Tomography) and MRI (Magnetic Resonance Imagery). The secured provision of Telemedicine CIS is critical of life safety.
- ***Logistics/Administrative*** Support is key to the success of civil and military crisis management operations. The activities include planning for personnel deployment and cargo movements, via a complex mix of air, sea and land routes; developing and managing cargo and asset tracking information; procurement and purchasing systems both in theatre and at the rear echelons. GOVSATCOM Crisis Management service shall support Information Systems supporting Logistic and Administrative workflows.
- ***Welfare*** is the provision of communication services to support private communication to deployed personnel. It comprises a range of services such as email, video

[5] These services are further detailed in chapter 10.3

conferencing and web browsing which can be consumed from either fixed or wireless devices. The provision of welfare services is an important element to support.

- ***Surveillance:*** GOVSATCOM Crisis Management Services shall support Surveillance missions as described in chapter 8 within the Crisis Management Area.

Time Constraints

The GOVSATCOM crisis management Service should be made available under the following conditions:

- Either first responder are prepositioned with compatible terminals on the mission area described in 7.2, then the GOVSATCOM services should be made available **less than twelve hours** after the decision is made to provide the GOVSATCOM crisis management service over the specific area.
- If not, the GOVSATCOM services should be made available **less than forty eight hours** after the decision is made to provide the GOVSATCOM crisis management service over the specific area. The time to deploy terminal equipment (including transport if they are not locally available) must be included in this delay.

The GOVSATCOM service shall remain operational as long as the situation requires the presence of the above first responders and no terrestrial means of communication can substitute the GOVSATCOM service. In particular for the specific case of CSDP operation in line with the European Level of Ambition a duration of up to two years can be anticipated.

Terminal needs

Different terminal equipment is needed depending on the crisis management mission phases and locations (i.e. extreme environmental conditions in the Arctic, deserts, or high seas).

When first responder teams reach the crisis area, tracking and hand-held SATCOM equipment is immediately needed. Such equipment should not require specific training or specific conditions to be deployed and/or operated.

Additional Very Small Aperture Terminals and plug-and-play SATCOM terminals may be deployed to enable both reception and transmission of larger quantity of information.

The topology of the communication networks may evolve: mobile communication may be locally ensured via deployed radio networks, so interoperability with radio equipment is needed.

This terminal equipment can be pre-positioned with the various users or can be deployed when the GOVSATCOM service is being delivered (c.f. 7.5)

GOVSATCOM Services for surveillance

Border surveillance missions in the context of Eurosur [19] or maritime awareness [20] for which military forces are involved along with other civilian security actors require Intelligence Surveillance Reconnaissance (ISR) capabilities (a range of sensors collecting intelligence to inform decision making). Connecting the various surveillance platforms and distributing relevant information to the relevant actors when and where needed is one of the greatest challenges to which an EU GOVSATCOM service could contribute.

Governmental users benefiting from the Service

This service should be made available to

- Land border surveillance , to connect Homebase, national authorities and Frontex to mobile patrol assets and teams when deployed beyond the range of terrestrial radio links
- Maritime surveillance including border control, fight against illegal immigration, general law enforcement, search and rescue, pollution detection and response environmental monitoring, ports and vessel monitoring, AIS, SAR, fisheries control as well as civil CSDP missions and operations at sea.
- Specific Military operations (EU or national)

Mission area and communication path

Two types of user areas can be considered

1. A global coverage with a scattered density of surveillance assets

A local coverage over areas of more intense density of surveillance assets which dimensions are in the order of few thousand square kilometres

Supported communication services, platform, terminal type

These services should be used to transmit

- Short Video on the move
- Voice (fixed and on the move)
- High resolution Radar and Optical Images transmission (fixed and on the move)
- Broadcast and Multicast data services (fixed and on the move)
- Low data rate systems (fixed and on the move)
- Remote and secured access to specific information systems

Mission Location

The local coverage GOVSATCOM maritime surveillance service shall cover specifically

- The Mediterranean and Black Sea
- The North and South Atlantic

- The Baltic area (the specificity of the Arctic region is addressed in chapter 10.1.)

The local coverage GOVSATCOM land border surveillance service shall cover specifically external EU frontiers. A specific coverage provision should be considered in order to cover possible new adhesion to EU within the GOVSATCOM lifetime.

Time Constraints

Near real time

The evolution of a surveillance missions implies the need for a very rapid reaction time between the detection of a security incident and the intervention of a response team.

In order to meet this objective GOVSATCOM service should allow real time connectivity between the surveillance platforms which are not connected to terrestrial infrastructures and the intervention units with sufficient bandwidth to transmit and receive the above communication services.

Among the surveillance assets which could benefit GOVSATCOM services specific solutions should be developed to address air breathing platforms, remotely piloted systems and earth observation satellites which are becoming indispensable to complement other types of patrolling systems which can directly intervene when an incident is detected.

Permanent Coverage

The GOVSATCOM coverage of a surveillance area needs to be permanent, with in some cases enhanced surveillance in the case of a crisis situation (see Chapter 7).

Terminal needs

The terminal used for surveillance mission should be used for the two types of coverage foreseen in 8.2. They should allow **high data rate links with and between remote ground stations.**

. Response teams involved in surveillance mission are likely to operate in a crisis management situation and therefore should also allow for the type of environment described in 7.

The main feature of the GOVSATCOM terminals for surveillance is their integration in the various surveillance platforms. These requirement should be addressed at the early stages of system design and should take into account

- the specificities of the platforms (operating environment, mass, electric, consumption aerodynamics etc.)
- The need to decouple the terminal from the GOVSATCOM service as described in 6.1 and 6.2.

GOVSATCOM Services in support of key infrastructure management

The provision of GOVSATCOM services can be required to support major infrastructures where the absence of proper communication links can be detrimental to the security and safety of the EU, the Member States and its citizen.

Some of the infrastructure listed below required immediate support of GOVSATCOM services. For some other infrastructure, the need for SATCOM is already established, but further analysis is requested to assess the need for a specific GOVSATCOM services. For other infrastructures, although it is clear that communication are critical, the final choice of the technological option (space or ground based communication) is not yet made. Finally some infrastructures that are not listed below could also benefit an EU GOVSATCOM service if and when available.

Therefore the family of GOVSATCOM services must be further studied on a case by case basis to decide the relevance of a GOVSATCOM service and precise the type of GOVSATCOM requirement which could meet the user needs described in the following sections.

But even before such analysis is being conducted, an agreed scope and definition and possibly a framework for EU GOVSATCOM services could help the discussion at EU and/or national level regarding the design or the evolution of the information systems corresponding to these candidate infrastructures.

Diplomatic Networks and Humanitarian Aid

Assured and secured communications are a key requirement for European and national diplomatic networks. Recourse to SATCOM solutions is necessary to complement the usual means of telecommunication with a solution independent from the hosting States communication networks. In addition the consular networks and the local offices responsible for humanitarian aid are usually the first elements in place to organize a crisis response and to offer assistance EU Citizen's abroad.

GOVSATCOM service will offer such communication a level of the resilience corresponding to the level of Information assurance needed.

This demand is increasing with the evolution of the diplomatic needs in Europe:

- The Diplomatic Networks constitute an infrastructure which is more and more interlinked because EU Member States are looking for synergies and economies of scale.
- Since the creation of the European External Action Service, the EU maintains its own infrastructure of 139 Missions and Delegations around the word with several EU High Representatives and Special Envoys representing the EU across the world. They must rely on trusted and guaranteed communication network to function.
- In addition DG ECHO of the Commission connects 49 field offices and Member States entertain similar types of Networks.
- EU Member States have the same constraints at national level and are exploring common solution to maintain their diplomatic "footprint" while the Ministries of

Foreign Affairs (MFA) and those responsible for Cooperation are facing budget restrictions.

- The EEAS and DG ECHO are now requiring these kinds of Communications to liaise with the EU Delegation worldwide and also to provide quickly deployable solutions for special envoys and high representatives. (see 7)

Diplomatic Networks of the EU and of Member States should constitute a primary user of future EU GOVSATCOM services.

Space infrastructures

"Space assets have become indispensable for our economy and… their security must thus be ensured" [21] . This statement extracted from the Council Resolution of 26 September 2008 can be applied to the EU which is responsible for the space infrastructures Copernicus Galileo. But other national and European space infrastructures including Copernicus contributing missions, and space infrastructures operated by ESA and EUMETSAT and the Space Surveillance and Tracking (SST) Framework should also benefit such protection.

Space infrastructure has two different usage of satellite communication:

1 to distribute the space services to the final users:

The EU -EGNOS systems augment the GNSS signals and provide it to users in the EU. This application is particularly critical for aviation.

Another example is the EUMETCAST network for EUMETSAT weather data and in the future Copernicus Services.

2 as part of the infrastructure itself

Some space infrastructures rely on secured satellite communication to ensure the information exchanges necessary for the functioning of the system

For instance to ensure a proper functioning the operations of Galileo require secure communication between the monitoring station distributed in EU territories across the globe. The level of protection of those communications needs to be commensurate with the level of security of the most critical service of Galileo: the Public Regulated Service

Copernicus uses a data relay service (EDRS) based on optical satellite communication links. Those links can ensure near real time transmissions and are very resilient to jamming and interception.

For each space infrastructure an analysis should be conducted to assess and possibly define the GOVSATCOM services which would best contribute to increase the security of space infrastructures while responding to some of the needs described in the above chapters.[6]

Aviation

There is growing dependence in the aviation industry on satellite communications.

[6] In particular to support crisis management and surveillance as described in chapters 7 and 8

This dependence will be affected notably by the development of new services for which the reliance of SATCOM is both

- critical as it may have impact of the safety and security of both transported passenger and inhabitant affected in case of a crash
- a governmental responsibility in accordance with ICAO provisions and the ensuing EU law.

Both civil and governmental aviation require satellite communications tailored to their specific needs. Some of those needs may be best met by GOVSATCOM solutions.

The following specific aviation services have been identified for potential future GOVSATCOM services applications:

AIR TRAFFIC MANAGEMENT (ATM)

Air Traffic Management is being progressively renewed to meet both the increased air traffic and the new environmental constraints. Systematic use of Global Navigation Satellite Systems (GNSS) such as GPS or Galileo, coupled with advanced communication techniques using SATCOMs is contributing to an increased automation of ATM.

In Europe, as part of the Single European Sky ATM Research (SESAR), the Future Communications Infrastructure for aviation will define and validate the future SATCOM solution for ATM. A fundamental aspect of the SESAR concept is the greater integration of the aircraft into the Air Traffic Systems and increased use of data sharing between the aircraft and the ground systems to enable trajectory based operations. To enable this SESAR is proposing the “multilink concept" in which SATCOM will play an important role alongside terrestrial based communications. The communications between the aircraft in-flight and the ground control centres are critical for the safety of the flights: they should be secured against ill-intentioned acts. Standards are defined by ICAO globally and by EASA at European level. Their need and potential provision (including certification) is evaluated in the context of the Single European Sky, in particular the SESAR project.

Global Flight Tracking

Following recent aviation incidents, several studies (ICAO, SESAR, etc.) are analysing the permanent tracking of the aircraft in-flight anywhere in the world. In February 2015, the ICAO high-level safety conference decided that all aircraft position should be tracked at least every 15 minutes when there is no emergency situation; the position update rate is changed to around 1 minute when an abnormal event is detected. The European Commission published in December 2015 a regulation [22] which mandates the global flight tracking

Such services entail information assurance requirements which could benefit from the information assurance provided by GOVSATCOM services.

Land based transportation systems

As it is the case with aviation, the evolution of Radio communication and Positioning will enable rapid evolutions towards faster cheaper safer and greener land transport systems.

But public authorities at EU, National and Local Level will keep a responsibility in the safety and security of land based transportation Networks. These Critical Infrastructures become

increasingly vulnerable because of their reliance on communication networks (Terrestrial or Space based). In this context GOVSATCOM services could complement and in some cases substitute terrestrial radio Networks to ensure the safety and security of the critical communication associated with the operations of these transport networks.

The following land transportation projects have been identified for potential future GOVSATCOM services applications:

Rail Traffic Management

European Rail Traffic Management System (ERTMS) [23] is an initiative supported by the European Union to greatly enhance safety, increase efficiency of trains and enhance cross-border interoperability of rail transport in Europe by replacing the national signalling systems by creating a single Europe-wide standard for train control and command systems.

ERTMS essentially uses ground-based radio communications via GSM Network. Both SATNAV[7] and GOVSATCOM services could increase the capacity and resilience of future evolutions of the railway communication system. Research and development activities on satellite positioning technologies are included in the context of the Shift2Rail Joint Undertaking.

Intelligent Transport Systems

The development of intelligent terrestrial vehicles, cars, trucks, ships, barges, as well as automated road transport and automated ships/barges is currently subject to a number of studies and experiments world-wide.

These Intelligent Transport Systems (ATS) will require very dependable communication links, either with other vehicles or with the ground infrastructure.

It is possible that they will require satellite communications where ground-based systems are not available and the Intelligent Transport System program currently coordinating these studies.

The interoperability of these systems will be based on common standards since the communication links are highly critical for safety and must be secured. A Specific GOVSATCOM service could be envisaged in the future to support the deployment of future ITS.

[7] Navigation satellites, i.e. GPS or Galileo

GOVSATCOM services for specific use-cases

This chapter describes specific use-cases that require particular attention because they correspond to an identified gap and are linked to a political/technology priority for which the deployment of a proper secure SATCOM technology could be a key enabler.

As for chapter 9, further analysis is needed to assess the need for specific GOVSATCOM services and the choice of the technological options.

Specific user needs related to the Arctic Region

Sustainable economic development faces specific challenges in the Arctic region. Compared with other parts of Europe, the European part of the Arctic has a sparse population spread over a wide area and is characterised by a lack of transport links, such as road, rail or east-west flight connections. The wider Arctic region is rich in natural resources such as fish, minerals, oil and gas. The lack of terrestrial communications means that space infrastructure has an increasingly important role to play in connecting people and businesses, and meeting the educational, health, linguistic and cultural needs of Arctic communities

Satellite Telecommunication needs cannot be adequately met with the present mainly equatorial orbit satellites. [11]

Specific attention must be paid to the Arctic region part of several of the below needs:

- The Arctic region must be covered by GOVSATCOM surveillance service of chapter 9.
- The diplomatic activity calls for GOVSATCOM means (see chapter 9.1) ;
- The Arctic region is very important to monitor space infrastructure. Both Copernicus and Galileo have monitoring and control station close to the Arctic area. (see chapter 10.4);
- Many air traffic route cross the Arctic area, Arctic coverage would be a requirement of a future GOVSATCOM service for aviation (see chapter9.3);
- Surveillance and Crisis Management missions may take place in the Arctic as human activity develops (see chapters 7 and 9).

Remotely Piloted Aircraft Systems (RPAS)

RPAS are likely to play a significant role for future surveillance mission as described in 9 and they are also closely related to the evolution of Aviation needs of paragraph 9.3.

They will be used for Surveillance missions both in the context of crisis management, pre frontier surveillance and maritime surveillance and are likely to meet other governmental needs as the technology develops.

Most of the long range at lower altitudes, medium (MALE) and high altitude RPAS (HALE) require Beyond Line of Sight (BLOS) communication which can only be achieved through satellite communication links.

Although they can use the same communication channel; there are two distinct types of Satellite communications to be considered, one related to the RPAS operation (CNPC) and one related to its payload (sensor data transfer):

1 The Command and Non-Payload Communications link of the platform

This link used to pilot the platform and its integration within the Air Traffic Management system is critical both to perform the mission but also to prevent any damage resulting from the loss of control of a ton class aircraft.

Usually the Command and Control platform link has a limited bandwidth with a very robust waveform.

.

It will have to meet the aviation standards described in 9.3and in particular the regulatory framework under development relative to RPAS integration in civil airspace

2 The download link (and control) link of the payload(s)

Depending on the criticality of the mission this link can be protected or not and therefore be channelled either through a GOVSATCOM or a COMSATCOM service.

With regards to the RPAS payload communications, GOVSATCOM shall support the relatively high bandwidth return links (i.e. from the RPAS to the data analysis centre) which will be used during future ISR missions. In addition, the need for payload control shall be supported by GOVSATCOM.

Machine to Machine (M2M) and low data rate applications

There is an emerging user requirement for low data rate applications which correspond to a big variety of new applications related to M2M communications and to the "Internet of Things (IoT)". These applications communicate with very short data messages which size is not well suited for most communication networks designed for high bandwidth and massive data transmission. This M2M/IoT communication will require both terrestrial and space communications to connect objects anywhere any place.

Future 5G networks will address these specific concerns for general public MDM/IoT applications, but they will not address the specific security concerns of Governmental Users.

Security actors and infrastructure have a critical need for robust and secure M2M which would not rely only on terrestrial infrastructures. Examples of such services include maritime safety applications, event detection and alerting via in-situ sensors used in the context of border protection, non-cooperative tracking of people vehicles and equipment in the context of police and law enforcement missions and operations, natural and industrial hazards monitoring for civil protection, ATM messaging, Global Flight Tracking (see 9.3), TT&C transponders of RPAS etc.

Such secured M2M application when using High data rate GOVSATCOM services lack spectrum efficiency which impacts negatively the price for the users. Specific solutions need to be developed to offer dedicated secured and cost-effective GOVSATCOM services for M2M.

Appendix

Definitions

a) **Information Assurance:** Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. [18]

b) **Artic:** Artic region covers the area around the North Pole north of the Arctic Circle. It includes the Arctic Ocean and territories of the eight Arctic states: Canada, The Kingdom of Denmark, Finland, Iceland, Norway, Russia, Sweden and the United States. The Arctic region also includes the Arctic Ocean and its adjacent seas. [11]

   For the purpose of this document the Artic will be considered as the area that is not well covered by Geostationary SATCOM satellite services.

c) **SATCOM service**: A communication service offered by satellite(s), which channel(s) relay(s) and amplify(ies) communication signals between a source and a receiver.[8]

d) **Third Party:** a State or an organization that is not Member of, nor belongs to the EU

e) **Waveform:**

   - The set of transformations applied to information to be transmitted and the corresponding set of transformations to convert received signals back to their information content.
   - Representation of a signal in space
   - The representation of transmitted RF signal plus optional additional radio functions up to and including all network layers.

   (Examples of civilian radio waveform include GSM, UMTS, DVBs, DVBt, 4G, 5G, TetraPol etc.)

   Software Defined Radio (SDR) technology aims at implementing several waveforms into an SDR terminal via a simple description of the software files describing the waveform and its characteristics.

Bibliography

[1] International Telcommunication Union, Radio Regulations, 2012.

[2] European Council, “European Council 19/20 December 2013 Conclusions”.

[3] EU Council, «Council conclusions on "Underpinning the European space renaissance: orientations and future challenges"».

[8] The ITU RR defines "space radio communication" as any radio communication involving the use of one or more space stations or the use of one or more reflecting satellites or other objects in space.

[4] European Commission, “Work Programme 2016,” [Online]. Available: https://ec.europa.eu/priorities/work-programme-2016_en.

[5] European Defence Agency, «Common Staff Target on Governmental Satellite Communications (GOVSATCOM) 2020-2025».

[6] European Parliament , «Resolution on space capabilities for European security and defence».

[7] E. U. “Global Stratgey,” 2016. [Online]. Available: https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union.

[8] F. Mogherini, H. R. o. t. U. f. F. A. and Security Policy, Vice-President of the European Commission et Head of the European, *Implementation Plan on Security and Defence,* 2016.

[9] European Commission and European External Action Servce , “Joint Framework on countering hybrid threats a European Union response,” 2016.

[10] General Secretariat of the Council, «European Union Maritime Security Strategy,» 2014.

[11] European Commission and the High Representative of the Union for foreign affairs and security policy, *An integrated European Union policy for the Arctic.*

[12] European Commission, *Space Strategy for Europe,* European Commission, 2016.

[13] European Commission, *European Defence Action Plan.*

[14] C. J. Jean and P. o. t. European Commission , “State of the Union 2016,” European Commission, 2016.

[15] E. Commission, «INCEPTION IMPACT ASSESSMENT Governmental Satellite Communications (GOVSATCOM),» 2016. [En ligne]. Available: http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_grow_002_govsatcom_en.pdf.

[16] European Commission and the High Representative of the Union for foreign affairs and security policy, «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace».

[17] The European Parliament and the Council, *DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.*

[18] EU Council, *COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information.*

[19] E. Commission, «EUROSUR,» [En ligne]. Available: http://ec.europa.eu/dgs/home-affairs/e-library/docs/infographics/eurosur/eurosur_en.pdf.

[20] European Commission et European External Action Service , «JOINT STAFF WORKING DOCUMENT On the implementation of the EU Maritime Security Strategy Action Plan,»

2016.

[21] EU Council , Council Resolution of 26 September 2008 ‘Taking forward the European Space Policy’, p. 5.

[22] European Commission, *COMMISSION REGULATION (EU) 2015/2338 of 11 December 2015 amending Regulation (EU) No 965/2012 as regards requirements for flight recorders, underwater locating devices and aircraft tracking systems.*

[23] European Commission , «ERTMS - European Rail Traffic Management System,» [En ligne]. Available: http://ec.europa.eu/transport/modes/rail/ertms/index_en.htm.

[24] United States Government Accountability Office, «Defense Satellite Communications: DOD needs additional information to improve procurements,» 2015.

[25] International Telecommunication Union, Radio Regulations, 2012.

List of abbreviations

AIS	Automatic Identification System
ATM	Air Traffic Management
BLOS	Beyond Line of Sight
C2	Command and Control
CNPC	Command and Non-Payload Communications
COMSATCOM	Commercial Satellite Communications (on the global open market)
CSDP	Common Security and Defence Policy
CST	Common Staff Target
DG ECHO	European Commission's Humanitarian Aid and Civil Protection department
EASA	European Aviation Safety Agency
EDA	European Defence Agency
EDRS	European Data Relay Satellite System
EEAS	European External Action Service
EGNOS	European Geostationary Navigation Overlay Service
EGNSS	European GNSS (EGNOS and Galileo)
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
EU	European Union
EUCI	EU Classified Information
EUMETCAST	Data dissemination systems of EUMETSAT Data
EUMETSAT	European Organisation for the Exploitation of Meteorological

	Satellites
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GOVSATCOM	Governmental Satellite Communications
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HALE	High Altitude Long Endurance (RPAS)
ICAO	International Civil Aviation Organization
IER	Information Exchange Requirement
ISR	Intelligence Surveillance Reconnaissance
IoT	Internet of Thinks
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
LEO	Low Earth Orbit
LSS	"link status" service
MALE	Medium Altitude Long Endurance (RPAS)
MEO	Medium Earth Orbit
MILSATCOM	Military Satellite Communication
M2M	Machine to Machine (Communication)
NGO	Non-Governmental Organization
NIS	Networks and Information Systems
NSA	National Security Agency(ies)
PSTN	Public Switched Telephone Network
RPAS	Remotely Piloted Aircraft System
RR	Radio Regulation (of the ITU)
S2R	Shift to Rail
SAR	Search And Rescue
SATCOM	Satellite Communication
SATNAV	Satellite Navigation
SESAR	Single European Sky ATM Research
SST	Space Surveillance and Tracking
SWIM	System Wide Information management
TT&C	Telemetry, Tracking, and Command

UC	User Communities
VSAT	Very Small Aperture Terminal (Satellite terminal with an antenna size around 1 meter)