Cyber Resilience

→ UNITED SPACE IN EUROPE, UNITED EUROPE IN SPACE

ESA Cyber Resilience Team

BELSPO/ Brussels

30/09/2019

Space Safety and Security – Cyber Resilience

1. **ESA’s Mandate and Objectives**
2. **Two Pillar Approach**
3. **Procurement Approach**

CYBER SECURITY & ESA’S MANDATE

> “To provide for and promote, for exclusively peaceful purposes, cooperation among European states in **space research** and **technology** and their **space applications.**”
>
> ***Article 2 of ESA Convention***

→ Interpretation of the ESA Convention in 2003: “peaceful purposes” interpreted in light of UN treaties as “non-aggressive”.

- ❑ Cyber resilience is a fundamental element of ESA’s capacity to fulfil this mandate and elaborate secured programmes for its stakeholders
- ❑ ESA has a duty to protect its Member States’ investments in space
- ❑ ESA is not a security actor but provides secured systems, for its own missions and third party missions alike
- ❑ Cyber security market: USD 101 billion in 2017, 90% civilian, increased by 12% in 2018. The compound annual growth rate to be of 8.5% until 2022. Cyber security is thus a critical challenge to the further growth and competitiveness of European space industry.

SECURITY OBJECTIVES OF SPACE MISSIONS

Security Objectives

1. Data integrity
2. Data availability
3. Data confidentiality

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Typical Risks: Jamming, spoofing and hacking

- Communication networks:
  - Taking control of satellite
  - Attacks on ground infrastructure, control and data centres
- Unmanned platforms; UAV, cars, UUV, UMS…
- ISR platforms: Anti-jamming and spoofing protection
- Global system integration

➢ Increasing complexity with increasing entry points and vulnerabilities

➢ Major risk of backdoor holes in encryption and control systems (e.g. IoT)

➢ Challenges are the same whether the end users are civilian or defence entities (hence the purpose of this cooperation)

CYBER THREATS IN SPACE: AN EVERYDAY FACT

- Threats (cyber and hybrid) to governmental or commercial assets are now well documented (e.g. Russia's Luch/Olymp)
- ESA has a responsibility to protect its Member States' investments in space
- ESA needs to react to these threats; An increasingly holistic, comprehensive, visible approach is needed in:

1. Policy and regulatory matters;
2. Awareness and training;
3. Research and development;
4. Capacity building for operational cyber security.

CYBER RESILIENCE: STATE OF PLAY

New ESA Cyber Security Policy

- Improve cyber-security governance (cyber threat intelligence, cyber supervision and reaction)
- Develop and build preventative cyber-security measures
- Continue to identify and deploy reactive cyber-security solutions

A Comprehensive ESA Approach

- High level security risk analysis, identifying preliminary risk profile at corporate and space programme level;
- Supervision of the correct implementation of the ESA Security framework (Security Regulation and Directives), including preventative and reactive cyber security measures;
- Accreditation and certification of the space system granting resilience and robustness
- IT Cyber Policy
- IT corporate network monitoring and reaction with ESACERT
- IT detailed risk analysis,
- IT Security incident investigation and reaction
- ESA cyber operational awareness, exercises and trained via ESEC' cyber range;
- Specific System Engineering solution in Telecom, EoP and Navigation department;
- Transversal technology R&D activities and preparatory studies (e.g. with EDA), as well as some user-driven applications (secured satcoms, Quantum, etc.)

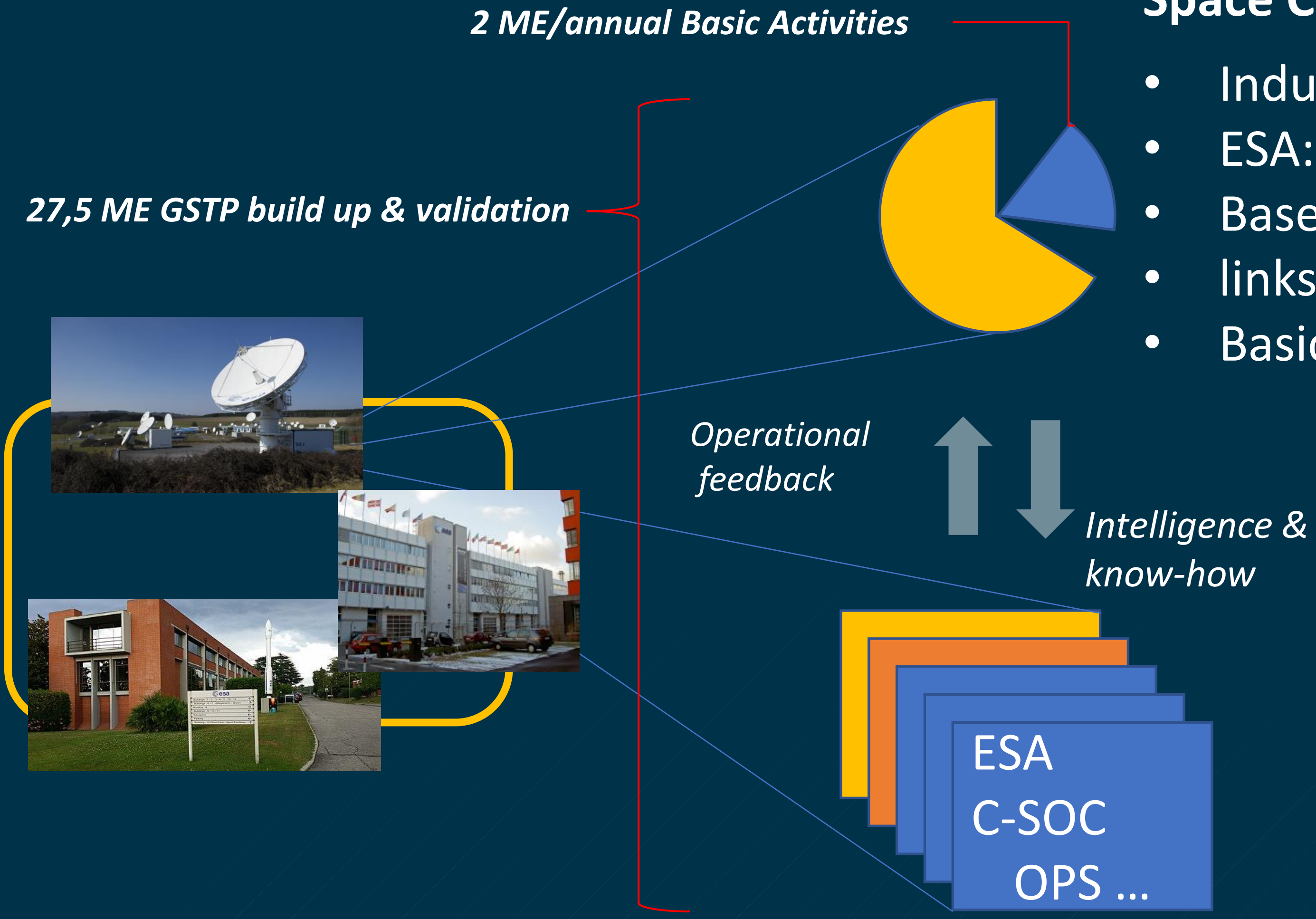
SPACE19+ CYBER RESILIENCE OBJECTIVES

- Protect ESA assets from cyber threats, whether intentional or accidental by setting up a capability that **expands / complements the existing functions of ESACERT** working in synergy with system-specific Security Operations Centres (e.g. Copernicus).

- Tackling this defining challenge requires adding a **Cyber Security Operations Centre** (C-SOC) for ESA mission operations, to monitor and protect IT and OT environments from attacks, protect space and ground segment as well as data exploitation. It further requires a holistic internal and external approach that will be undertaken by a **Space Cyber Security Centre of Excellence** (SCCoE)

- This initiative seeks to establish a **default capability at the disposal of the entire spectrum of ESA missions** that may not require the *ad hoc* development of a dedicated SOC system (e.g. Copernicus or Galileo) but whose security profiles may warrant specific cyber protection (elaborated through an integrated risk assessment, security-by-design development, and accreditation process).

CYBER RESILIENCE PROPOSAL FOR SPACE19+


2 ME/annual Basic Activities

27,5 ME GSTP build up & validation

Operational feedback

Intelligence & know-how

ESA

C-SOC

OPS …

Space Cyber Security Centre of Excellence (SCCoE)

- Industry-driven
- ESA: anchor customer
- Based on training/exercise/cyber range
- links to Cyber Security Centers throughout Europe
- Basic Activity for continuous operation

Space Cyber Safety & Security Monitoring Center(s)

- Builds on SCCoE
- ESA leads C-SOC; industry implements
- Supporting programmes
- Programmes to opt-in according to their needs
- GSTP for initial investment & start-up

PILLAR 1: SPACE CYBER CENTRE OF EXCELLENCE

- Mission: provide training, validation and test services, centralizing some forensic services/expertise as well as developing a distributed risk analysis process capability and legal analyses.
- Aim to ensure full integration of overall ESA activities into the wider cyber resilience efforts undertaken by Member States and in the EU.
- Based on the current ESEC Cyber Range, to be developed and operated by the ESA Security Office, through a multi service contract, staffed with ESA personnel supported by Seconded National Experts.
- Consolidating certain functions in the SCCoE will provide cost efficiencies and maximize available expertise, skills and resources for the benefit of all actors in ESA's Cyber resilience posture

- Expected Attributions:
  - ✓ Providing a synthetic environment to validate and qualify security operational procedure and system against cyber scenarios customized for user operational needs;
  - ✓ Providing a distributed security risk analysis and threat vulnerabilities process;
  - ✓ Implementing specific Cyber Security policies;
  - ✓ Testing technology and capability needs to ensure ESA resilience against future cyber threats;
  - ✓ Defining ESA's Cyber Resilience posture addressing e.g. corporate and operational networks under a common cyber security management framework.
  - ✓ Overseeing and complementing C-SOC functions, to support a unified cyber security goals.

PILLAR 2: CYBER SECURITY OPERATIONS CENTRE

- Mission: monitor and protect ESA's space and ground segment as well as data exploitation from cyber threats based on a holistic risk assessment approach.
- Will provide cyber security services to ESA customers according to their needs.
- To be developed under the authority of ESO in coordination with IT department and the Head of ESEC; to be operated by the IT department and located in ESEC. Key C-SOC interfaces and functional components would also be located at ESOC (interfacing NOC) and ESRIN (interfacing ESACERT, EOP SOC).

The C-SOC would offer such functionalities as:

- ✓ Corporate and mission critical monitor preventive & reactive network functions
- ✓ Threat and vulnerabilities risk analysis
- ✓ Sensors and technology data collection capability
- ✓ Analytics: correlation and triage of real-time data feeds, incorporating knowledge about ESA's environment, threats, and vulnerabilities, tier 1 for real-time (C-SOC) and tier 2 for in-depth analysis and alerting (SCCoE).
- ✓ Alerting: escalating incidents to customer (e.g. ESACERT, EOP) who have the operational authority to initiate the incident response
- ✓ Situational awareness and reporting: using cyber threat intelligence from a wide variety of sources, synthesising and feeding back as threat intelligence, and comprehensive reporting on cyber security status and performance metrics to the service customers and to SCCoE.

STUDIES – PREPARATION EFFORT

CSOC Studies

CSOC Studies – Demonstration projects

Secure Multi-Mission Ground Segment Study

1. **CSOC studies to collect ESA requirements and to scope the initiative in preparation of the programme proposal**
2. **Cyber resilience support to projects – pilot projects to engage with operational teams and demonstrate added value**
3. **sMMGS study to look at satellite to ground links and how to secure those**

PROCUREMENT APPROACH & SCHEDULE

- ESA is preparing two ITTs:

    1. To procure the SCCoE (B.A. & GSTP)
    2. To procure the C-SOC (GSTP)

- The procurement approach will be a one-stage, classified procurement.

- Tentative schedule: KO of contracts Q2 2020; qualification and accreditation reached by Q2/Q3 2023.

- Note that the GSTP is an optional ESA programme:
    - ✓ open to ESA Member States including Canada as a Cooperating State and Slovenia as an Associate State member.
    - ✓ Contracts are awarded based on *national support*, with the Participating States informing the Agency of their support to the Csoc activities *prior* to the issueing of an Invitation To Tender: if a Member State is not supporting the activity, its industry cannot bid.
    - ✓ Procurement generally occurs competitively on a 100% funding basis, although up to 50% or 75% ESA co-funding is possible in non-competitive tenders.

SPACE19+ FINANCIAL ENVELOPE PROPOSAL

1. A Basic Activity (BA) element of **2 M€** per annum to cover the SCCoE (over five years); B.A. are part of the Agency's Level of Resources (LoR) to which all ESA Member States contribute per GDP.

2. A GSTP element in competition to cover the design, development, initial roll out, validation and accreditation of a C-SOC for ESA (over five years) and partially the development of the SCCoE new functions.

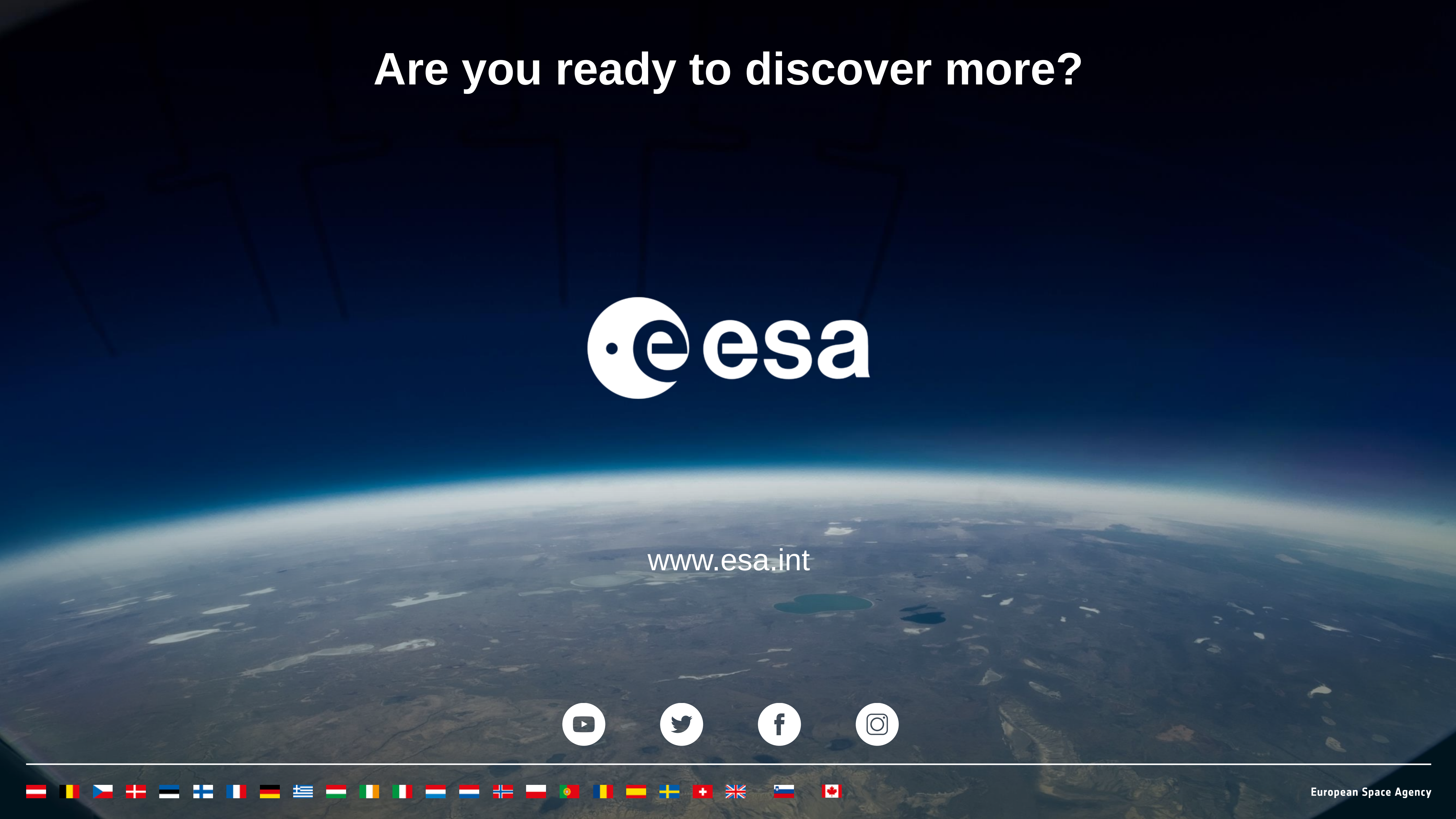
3. General and Administrative (G&A) budget component of **6 M€** to cover recurring costs for the provision of services during the period 2020 to 2024.

A proposal will be submitted for the continuous funding of the three activities at the following Council at Ministerial level.

PROPOSED SPACE19+ BUDGETS: RECAP

Year		2020	2021	2022	2023	2024	Total
B.A.	Cyber Range	2	2	2	2	2	10
GSTP	SOC	3.25	13.25	2.5	0.5	0.5	20.0
	IT	0.2	1.5	1.5	2.0	2.0	7.2
	Total	3.45	14.75	4.0	2.5	2.5	27.2
G & A		0.5	1.3	1.3	1.5	1.5	6.1

(M€ at 2019 e.c.)



Are you ready to discover more?

www.esa.int