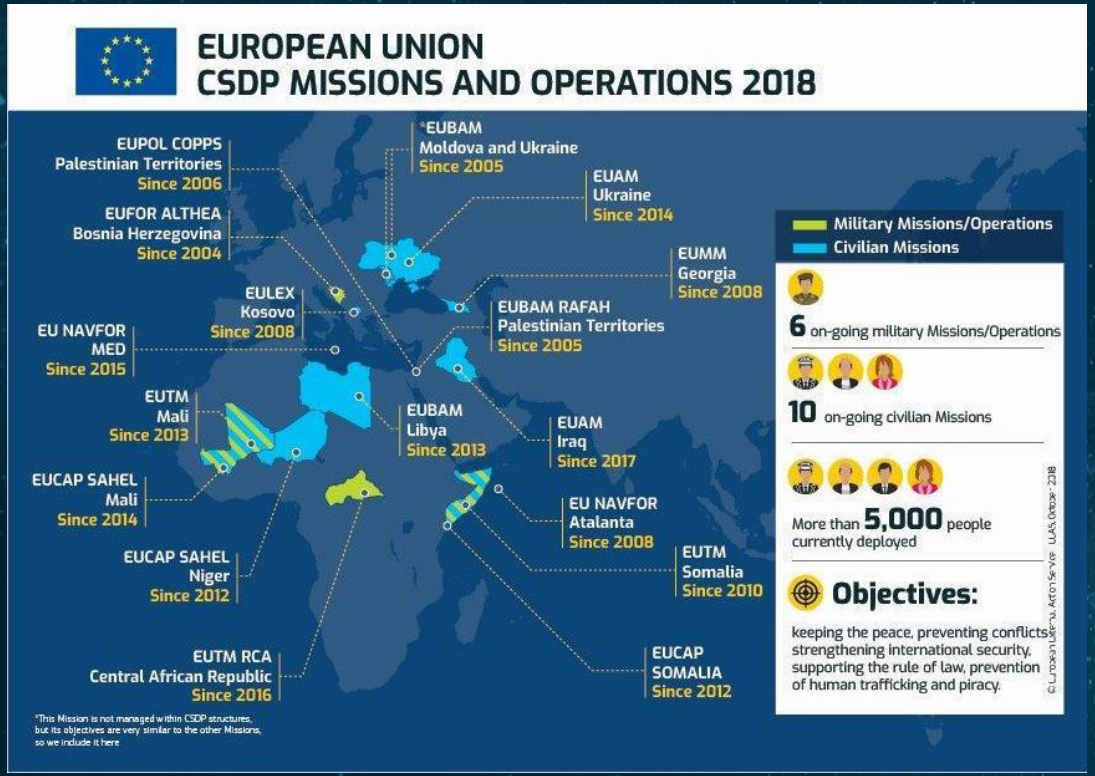
Joint ESA-EDA
Cyber Defence For Space project

CNES COMET
08 November 2021

SPACE: INDISPENSABLE TO EUROPE'S STRATEGIC AUTONOMY



- ✓ Information gathering
- ✓ Strategic analysis
- ✓ Political decision-making
- ✓ Operational implementation

"Space is an instrument for safety and security, diplomacy and soft power, development and international cooperation – a political necessity for a strong Europe as well as an important enabler of sustainable economic growth and stimulus." (Agenda 2025)

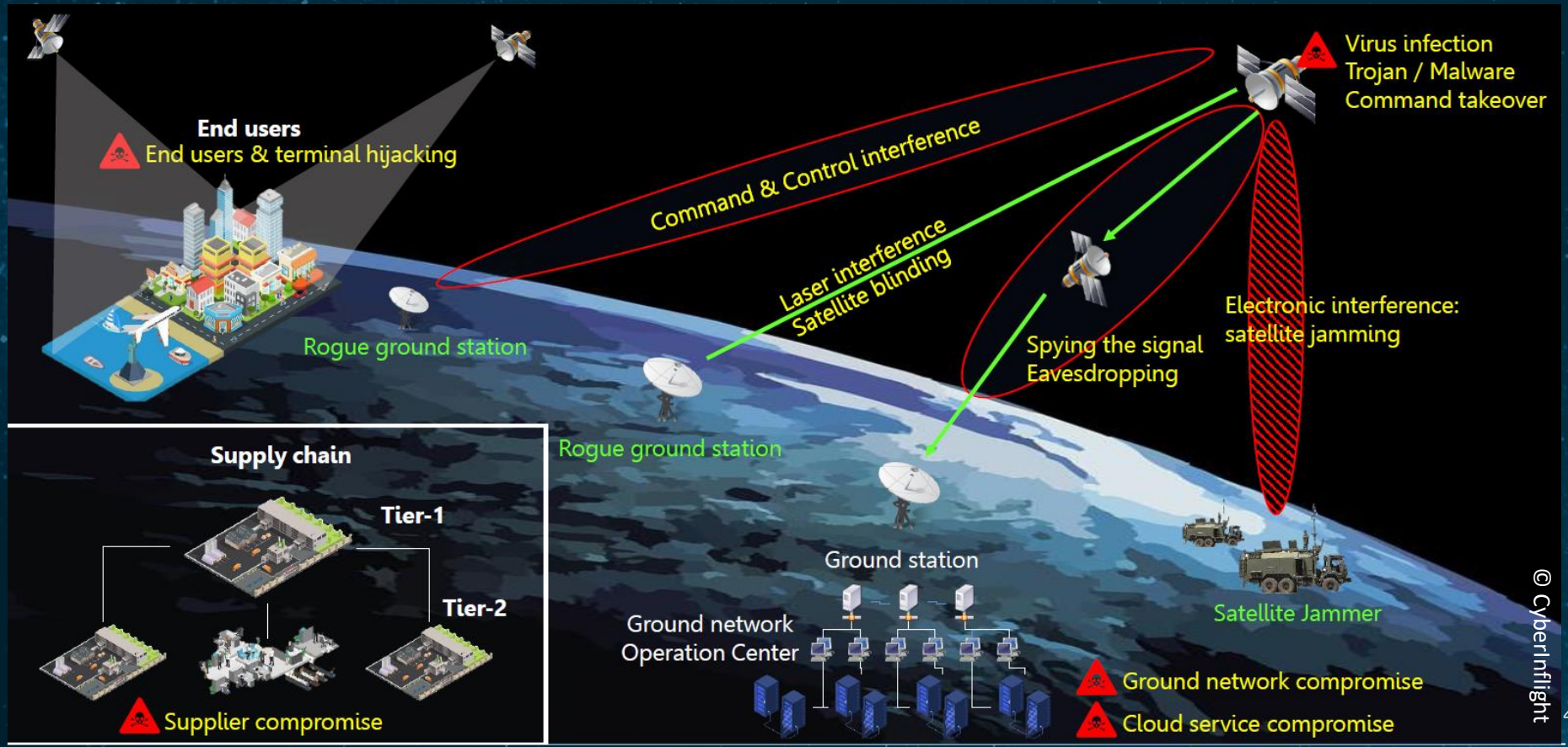
SPACE IN THE GLOBAL STRATEGY (JUNE 2016)

"In space, we will promote the autonomy and security of our space-based services… *European security hinges on better and shared assessments of internal and external threats and challenges. This requires investing in …* ***satellite communications, and autonomous access to space and permanent earth observation***."

The Implementation Plan on Security and Defence defines the capability efforts to be made: **cyber and maritime security, Intelligence, Surveillance and Reconnaissance (ISR), Remotely Piloted Aircraft Systems (RPAS), satellite communications including Governmental Satellite Communications (GOVSATCOM), and autonomous access to space and permanent Earth observation**.

2021-2022: Strategic Compass

THREATS TO THE SPACE ECOSYSTEM



CYBER THREATS: A POLITICAL RECKONING

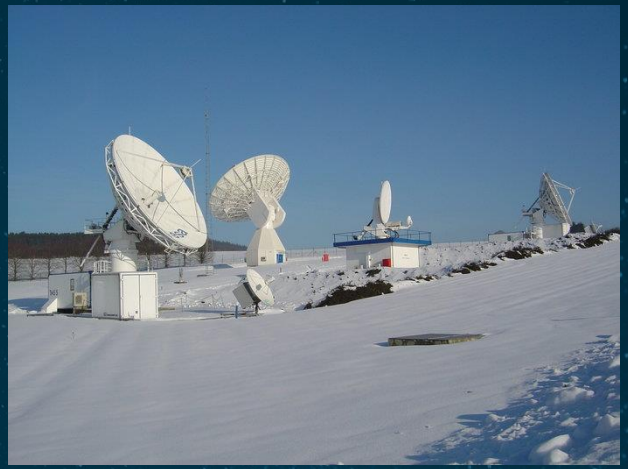
- European Council on 20 Defence 2013: cyber defence one of four key capability priorities
- 7 September 2018, the French Defence Minister publicly revealed that France's governmental satellite communication asset, Athena Fidus, had been spied on by the Russian Louch-Olymp satellite;
- September 2019: General Nick Carter, UK Chief of Staff: « Britain is at war very day » due to cyber
- The World Economic Forum's 2021 Global Risks Report puts extreme weather events and cybersecurity failures as the third and fourth most clear and present dangers to the world,.
- 11 March 2021: Laurence Parly, French Defence Minister: "France is ready to use cyber in attack mode"
- NATO Summit 13 June 2021: a key item was the US calling for reinforcing cyber and attribution
- 15 September 2021, European Commission President Ursula Van Der Leyen, in her State of the Union speech, announced a **European Cyber Defence Policy**, to be backed by a **European Cyber Resilience Act**

CYBER THREATS: A GLOBAL RESPONSE

- On 24 July 2020, the Commission presented its new EU Security Union Strategy 2020–2025 (COM(2020) 605 final): prominent presence of cyber resilience
- On 16 December 2020, the Commission published a cybersecurity package consisting of:
  - A new EU cybersecurity strategy;
  - A proposal for a revision of the Directive on ensuring a high level of security of network and information systems (so-called NIS Directive);
  - A proposal for a new Directive on the resilience of critical entities.
- 4 September 2020: U.S. Space Policy Directive 5 on Cybersecurity Principles for Space Systems, calls for U.S. space industry to adopt cybersecurity standards to protect data, IPRs; raises awareness on supply chains, industrial espionage, etc.: cyber security to be incorporated in all stages of space systems development and operations
- 14 June 2021 NATO Summit: Cyber one of the key messages, including attribution
- 15 June 2021 EU-US Summit (Statement Towards a renewed Transatlantic partnership): several items to increase cooperation to mitigate risks and increase resilience

CYBER THREATS: ESA'S CONTINUOUS RESPONSE

1. ESA CERT Routine Operations and OPS
2. Space19+:
   - ✓ Cyber Security Operations Center (ESEC, Redu, BE)
   - ✓ Cyber Security Center of Excellence (ESEC, Redu, BE)
3. ESA-EDA Cooperation
   - ✓ CD4Space Joint Study
     - ✓ Implementing Arrangement: 02 December 2016
     - ✓ Orientation workshops with Member States
     - ✓ Phase 2 on CTI just concluded
   - ✓ Cyber Ranges Federation MOU (10/12/2020) and Demonstration
   - ✓ Comprehensive Exchange of Letters 14 October 2021
4. Agenda 2025 Process towards 2022 Ministerial Council: « *ESA will develop European technological and commercial leadership in the areas of space traffic management, debris mitigation and removal, space weather, planetary defence, space logistics and* ***cyber resilience*** »



CYBER THREATS ARE NOW AN EVERYDAY FACT

- Threats (cyber and hybrid) to governmental or commercial assets are now well documented (e.g. Russia's Luch/Olymp eavesdropping on FR/IT Athena-Fidus)

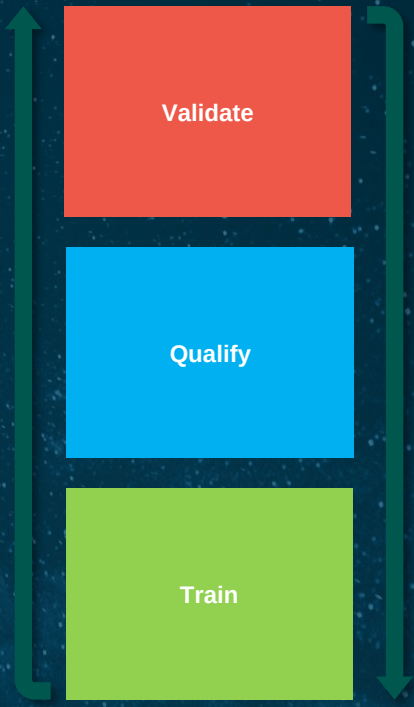
- ESA has a responsibility to protect its Member States' investments in space

- ESA needs to react to these threats and an increasingly holistic, coherent, visible approach needed in:

  - Policy and regulatory;
  - Awareness and training;
  - Research and development;
  - Capacity building for operational cyber security.

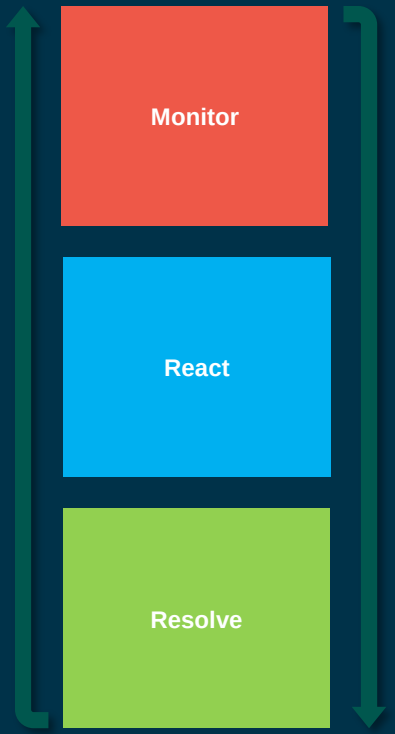
SECURITY CYBER CENTRE OF EXCELLENCE

- Security Cyber Centre of Excellence (SCCoE), an innovative tool, providing a unique capability in Europe. It will:
  - perform validation and testing of space systems through a synthetic environment, including the validation of security operating procedures and critical components, against up to date complex cyber threat scenarios.
  - Represent the focal point for a Security Information Sharing capability, training and centralisation of forensic services/expertise as well as developing a distributed risk analysis process capability;



ESA CYBER OPERATIONS CENTRE

- Cyber Security Operations Centre (C-SOC), complement the capabilities of our state-of-the-art Computer and Communications Emergency Response Team (CERT),
- The C-SOC will:
  - Provide an ESA-wide cyber monitoring and management capability.
  - Monitor and track relevant information and events with the objective of maintaining the overall Agency security posture.
  - Detect security incidents and support the readiness of the organisation's defensive capabilities.
- The C-SOC will be the ESA Super SOC coordinating all Cyber functionalities in ESA and representing an essential tool not only for ESA, but for all Member States and Third Parties.



ESA-EDA COOPERATION

- **Administrative Arrangement: 2011**
- **ESA and EDA can cooperate in any area of joint interest**
- **Secondment scheme**
- **Effective cooperation in technology, satcoms, RPAS, Cyber, CBRN**
- **EDA and ESA deepen cooperation on cyber resilience**

Areas of cooperation

Policy Cooperation

- Observer in C-Min and Space Council
- Coordination towards EC (and thus SWP/MS) and European Parliament (SEDE)
- DG-Level Bilaterals
- Space Dialogue (EEAS, EC, GSA, ESA)
- Public Relations, etc.

Ongoing Cooperation

- Critical Space Technologies
- GOVSATCOM
- **Cyber Ranges**
- **Cyber Defence R&T Study (2 phases)**
- CBRNe (AUDROS)
- Earth Observation - METEOR
- Unmanned systems (RPAS, UMS)
- GNC (ATENA)

Future & Potential Cooperation

- **Cyber Resilience (Joint Task Force)**
- Positioning, Navigation and Timing (PNT)
- Space and the Arctic
- New R&D demonstrations
- CBRNe Demonstration
- Next-Generation Secure Satellite Communication

CYBER RANGES FEDERATION

- On 28 June 2018, six EDA Member States (Austria, Belgium, Estonia, Finland, Germany and Latvia) signed a Memorandum of Understanding on the pooling and sharing of their respective cyber ranges capabilities.
- EDA and ESA on 29 November 2017 exchanged letters on a cooperation on cyber ranges and training in order to explore the objectives and framework for sustained cooperation, namely through this MoU.
- ESA undertaking to have the MoU approved by the June 2019 ESA Council, which would establish the legal link with the 8 EDA participating MS to cooperate on cyber ranges.
- Technical demonstration with the ESEC cyber range organised for November 2019
- ESA Party to the MOU since 10/12/2020

INSTITUTIONAL SETTING

+ Vice-President of the European Commission

JOSEP BORRELL
Head of EDA

+ High Representative of the Union for **Foreign Affairs** and **Security Policy**

Jiří Šedivý
EDA CHIEF EXECUTIVE

EDA STEERING BOARD
26 Defence Ministers

EUROPEAN DEFENCE AGENCY

GUIDELINES
REPORTS

FOREIGN AFFAIRS COUNCIL
Foreign /Defence Ministers

PSC
Ambassador level

CHODs

EUMC

EEAS
EUMS - CMPD

CONSULTATION & COOPERATION

FACTS & FIGURES

Only EU Agency whose Steering Board meets at ministerial level

26 Member States
(all EU members except Denmark)
Administrative Arrangements
with Norway, Serbia, Switzerland and Ukraine

Budget 2020
€36,5 Mio

EDA Portfolio:
ca. 300 activities related to capability development, R&T and defence industry

Value R&T projects 2004-2017 run within EDA:
approx. €1 billion

EDA / CapTech Cyber / TBBs overview

- TBB01 Cyber defence Situation Awareness
- TBB02 Cognitive Science with cyber implications
- TBB03 Exploring similarities and differences between cyber operations and Electronic Warfare
- TBB04 Cross-cutting Cyber defence for land, maritime, air and space
- TBB05 Protection of military CIS
- TBB06 Quantum computing and cryptography with cyber implications
- TBB07 Autonomous cyber response capabilities
- TBB08 Modelling and Simulation for Cyber defence

EDA / PROJECTS related to Cyber

The following projects are under work :

- Belong to CapTech Cyber
  - MASFAD II (Multi-agent system for APT detection) / pMS (BE, DE, NL)
  - CERERE (Cyber Electromagnetic Resilience Evaluation on Replicated Environment). pMS (DE, IT)

- Belong to different EDA directorate
  - CySAP RRP (Cyber Situation Awareness Packages - Rapid Research Prototype)
  - DCEC2 (Deployable Cyber Evidence Collection and Evaluation Capability) / Deployable kits for digital forensics.

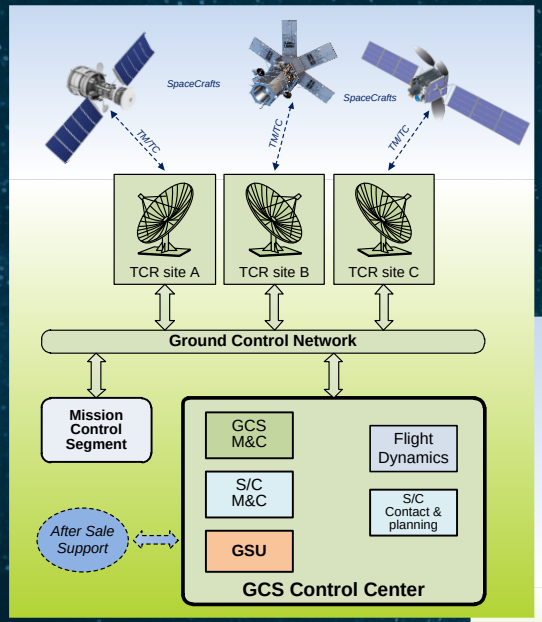
CD4SPACE

- Based on Critical Technologies for Non-Dependence (ESA, COM, EDA) rationale
- Implementing Arrangement: 02 December 2016
- 2 workshops with Member States supported the process in June 2017 and January 2019.
- The study is executed in 2 phases:
  - Phase 1 (12 months – 100 k€) for the identification of cyber threats on space missions and associated mitigation measures; 2 workshops with Member States supported the process in June 2017 and January 2019.
  - Phase 2 (12 months – 300 k€) for the development of the recommended solutions
  - Member States briefed between the 2 phases.

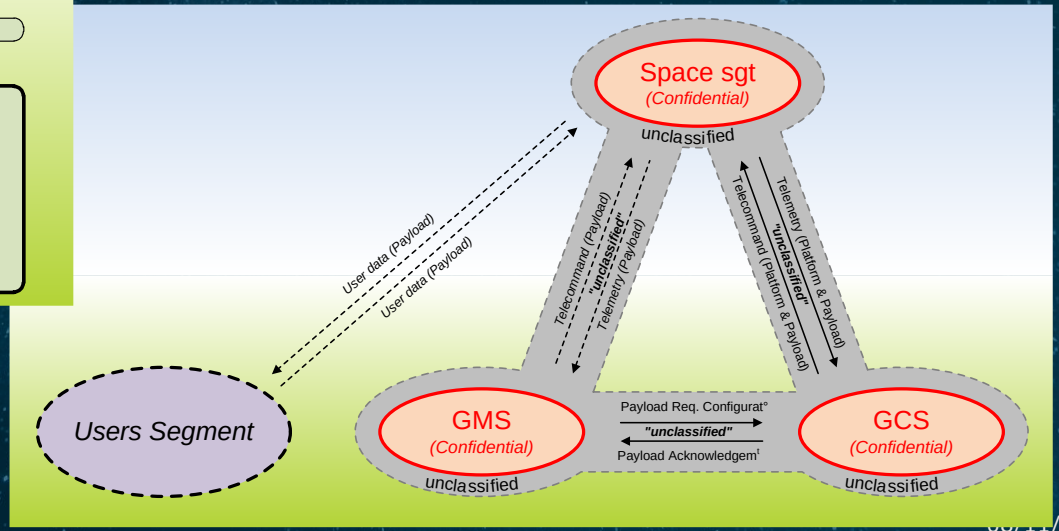
Objectives of the study

- **Phase 1**: Identification of vulnerabilities of inherent electronic components, signal and data processing, software and hardware elements along with communication links and protocols
- **Phase 2**: Cyber Threat Intelligence (CTI); webinar CTI exploitation demo on 30/09/2021

Common aspects for space missions



Typical case of architecture in defence context



CD4SPACE Phase 1

ID	Elementary Threat	A	E	D	Strategic	Terrorist	Hacker	Internal
ET_01	Data corruption			X	X	X	X	X
ET_02	Data leakage (Accidentally)	X						X
ET_03	Data leakage (Deliberately)			X				X
ET_04	Denial of ground network services			X	X	X	X	X
ET_05	Facilities malfunction							
ET_06	Ground facility physical at							
ET_07	Human errors							
ET_08	Interception of data							
ET_09	Jamming /Denial of servic							
ET_10	Interferences							
ET_11	Masquerade							
ET_12	Natural disasters							
ET_13	Replay							
ET_14	Software threats (Accider							
ET_15	Software threats (Delibera							
ET_16	System overload							
ET_17	Unauthorized access							
ET_18	Spacecraft physical attac							

Risk ID	Risk Title	Strategic Residual Risk Value	Terrorist Residual Risk Value	Hacker Residual Risk Value
RISK01	Lack of Space Situational Awareness & duty of care	medium	Negligible	Negligible
RISK02	Lack of non-repudiation evi the originator of an attack			
RISK03	APT and Malware infection			
RISK04	Denial of service attack			
RISK05	Insider attack			
RISK06	Supply chain attack			
RISK07	Attack during LEOP in clear			
RISK08	ILS satellite-in-the-middle a			
RISK09	Attack via EGSE before laun			

Title	Risk reduction impact	Return On Investment	Coordination interest (technical and financial efficiency)	Ranking
Cyber Threat Intelligence	****	***	****	1
Cyber Supervision	****	**	****	2
Security of Supply Chain	****	**	****	3
System hardening	****	**	***	4
Communication protection	***	**	**	5
Security Training	***	**	**	6
Program Resources	**	***	***	7
Penetration Tests	***	**	***	8
Space objects: Monitoring	**	**	****	9
EU NIS Directive	***	**	***	10
Certification scheme	**	***	***	11
Installation/Configuration Procedures	**	***	***	12
Access Control	***	**	*	13
Security of Remote Sites	***	**	*	14
Software-Defined Radio	***	**	*	15

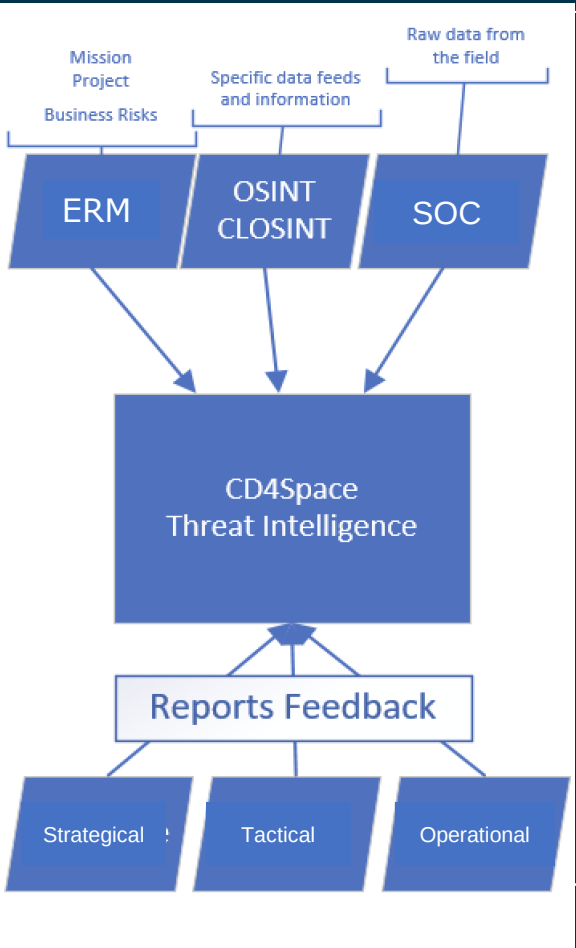
Phase 1: conclusions & way forward

- The report of the first phase has been released to ESA/EDA Member States end February; available to ESA Member States.
- On 17 January 2019, an intergovernmental workshop with ESA and EDA Member State representatives discussed its results and priority actions for implementation in Phase 2.
- Security Recommendations split in 3 categories:
  - Policy (procedure, doctrines…),
  - Technology , supply chain
  - Training
- For phase 2, and following Member State recommendations, the Executives agreed to implement the “Cyber Threat Intelligence” recommendation via a new tender:
- Other recommendations could be part of other funding proposals, e.g. CAT-B for specific security aspects or EDF or a new ESA-EDA joint project (e.g. on supply chain).

Cyber Defence for Space – Phase 2

- Identify the art-of-the-possible circa the use of CTI
- Contextualize Cyber Threat Intelligence (CTI) for Space missions (civil & military)
- Develop a specific Adversary Model for the Space domain

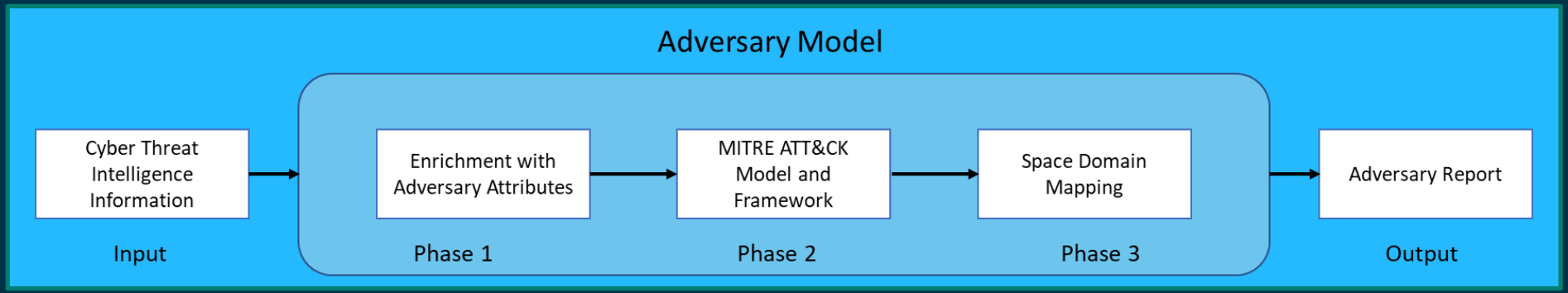
CTI Process



- ERM provides information on business, program , project risks (e.g. risk analysis on specific topic or mission or system)
- Data feeds provides information from OSINT or CLOSINT (e.g. known IoC for system in operation)
- SOC provides all the information coming from the field (events, incident, historical cyber security data, etc.)
- All the report recipient provides feedback on report (e.g. quality of information, level of details, etc.)

Space Adversary Model

- Defined a taxonomy of attributes to characterize attacks
- Extended the MITRE ATT&CK framework with specific TTP applicable to Space
- Space Map Matrix identifies threats across the Space Mission Phases (0 to Phase F) , Mission Types (Earth, Science, Communications, etc) and Mission Orbits (LEO, MEO, GEO, HEO, Inter-planetary)

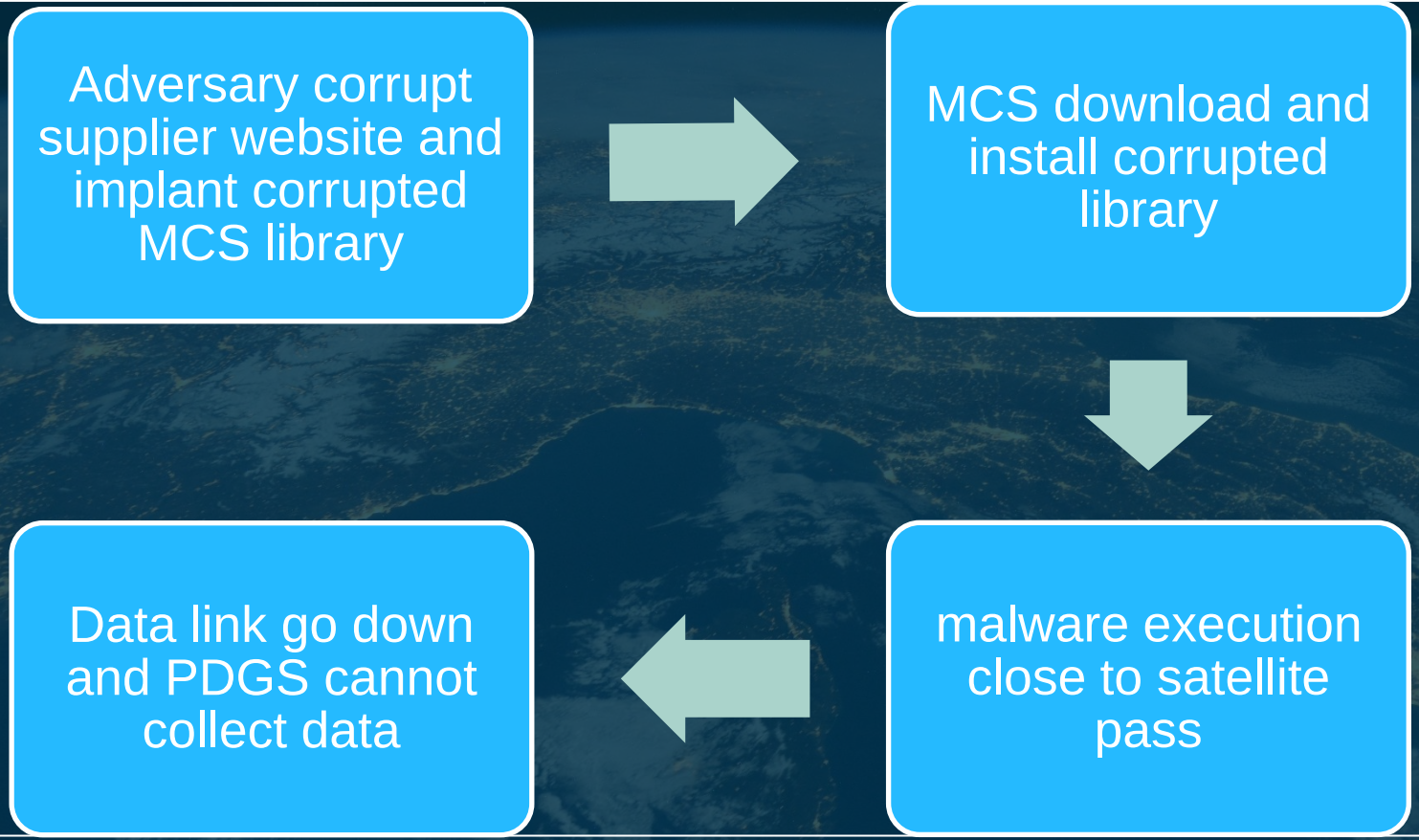


CTI for Space Simulation Scenarios

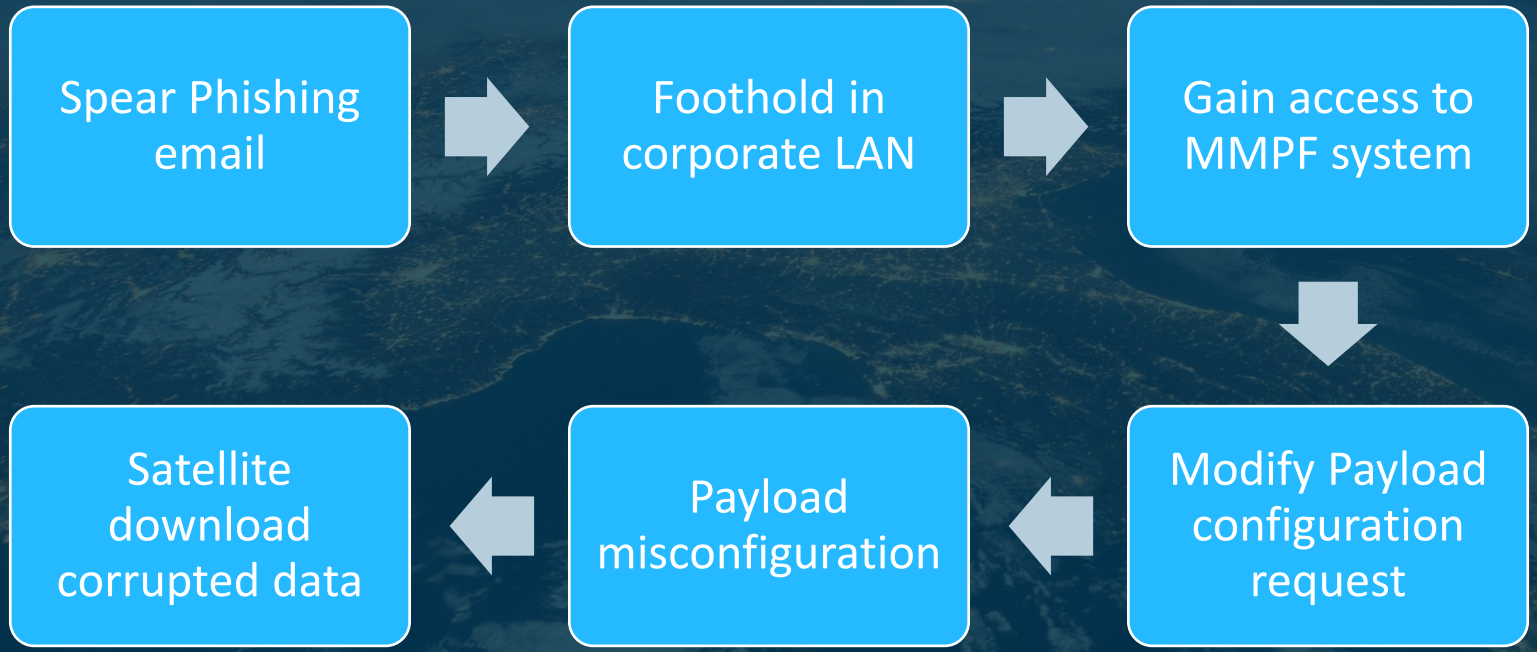
Concept:

- Two different scenarios
- Different attack vectors
- First wave of attacks without threat intelligence information
- Second wave of attacks with threat intelligence information
- Threat intelligence report for the two scenarios

Supply Chain Scenario



Spear Phishing e-mail scenario



Simulation Key Takeaways

Adversary Model

- Space elements have been captured by the model
- Playbook specific for the identified missions
- TTP and IoC correctly identified and implemented

Attack vectors

- Unauthorized access
- Supply chain
- Interception
- Denial of service

CTI demonstrate

- Capability of raising the cybersecurity posture of a space mission
- Effectiveness in improving Incident Response and in countering and blocking a cyber attack

Improvements

Further developing A.I. support to CTI

- Improve CTI production process
- Do automatic detection and recovery
- Reduce false positive
- Behavioural detection to improve early breach detection

THANK YOU !

Florent MAZURELLE
Principal Security Strategy Officer
Foresight, Strategy & Coordination Department
Director General's Services

Florent.Mazurelle@esa.int

John Irving
Cyber expert
ESA Security Office

John.Irving@esa.int

Patrick LANGLOIS
Project Officer CapTech Components
Technology & Innovation Unit
Research, Technology & Innovation Directorate

Patrick.langlois@eda.Europa.eu

Isidoros MONOGIOUDIS
Project Officer CapTech Communication Information Systems & Networks
Technology & Innovation Unit
Research, Technology & Innovation Directorate

isidoros.monogioudis@eda.europa.eu

Visit

www.esa.int

www.eda.europa.eu