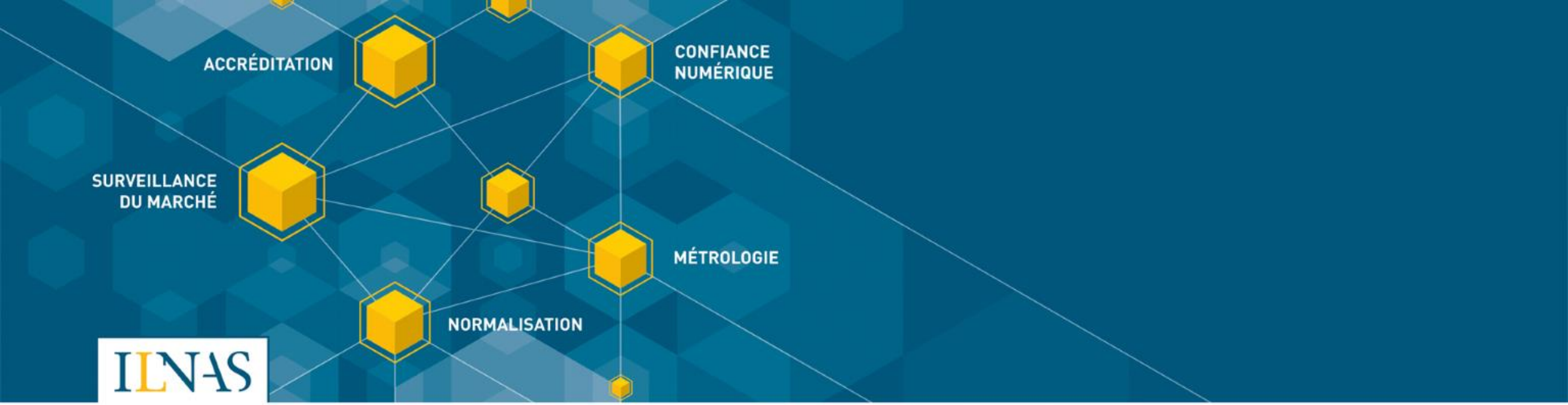
Welcome words by ILNAS

Dr. Jean-Philippe HUMBERT
Deputy Director – ILNAS



Workshop – Technical Standardization in Space and Cybersecurity

Welcome Words

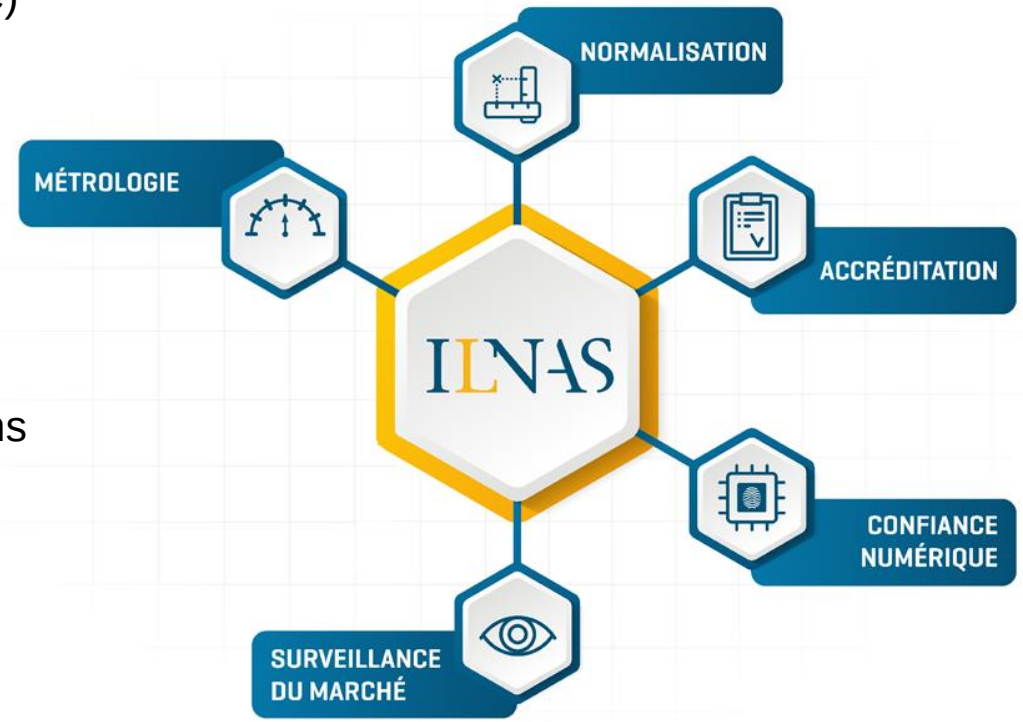
27th June 2023

Jean-Philippe HUMBERT - Deputy Director, ILNAS

I - Presentation of ILNAS

- **ILNAS**
  - Public administration under the authority of the Minister of the Economy
  - Creation: Law of May 20, 2008
  - Legislation in force: amended Law of July 4, 2014 reorganizing ILNAS
  - Total staff: 61 (June 2023)
  - ISO 9001:2015 certification (Budget and administration department, OLN, Digital Trust department, Market surveillance department, BLM, OEC)

PORTAIL-QUALITE.LU
QUALITE·SECURITE·CONFORMITE
UNE INITIATIVE DE L'ILNAS



- **National Standards Body**
  - Composed of 7 persons
  - Close collaboration with the E.I.G. ANEC-N

- **Digital Trust department**
  - Composed of 6 persons

II - Presentation of the Digital Trust department

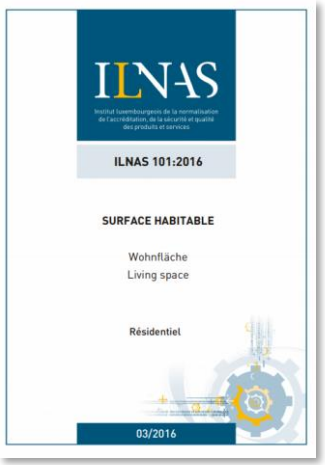
Main missions

- **National supervisory body for**
  - Trust service providers
  - Digitisation or e-archiving service providers (PSDCs – « Prestataires de Services de Dématérialisation ou de Conservation »)
- **Management and publication of Luxembourg's trusted list**
- **Member of the European Cybersecurity Certification Group ('ECCG') and National cybersecurity certification authority ('NCCA')**
- **Promotion of good practices**
- **National participant in the *European Multistakeholder platform on ICT Standardisation***

III - Presentation of the National Standards Body (*Organisme luxembourgeois de normalisation* – OLN)

Main missions

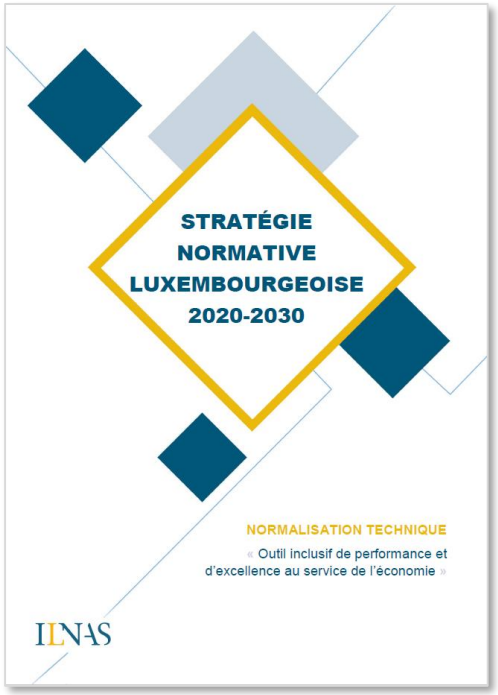
- Coordinate and supervise the creation of national standards
- Make standards available to the market
  - ILNAS eShop
  - ILNAS reading stations
- Manage the participation of national stakeholders in the international standardization organizations (ISO, IEC, CEN and CENELEC)
- Represent Luxembourg in the standardization related organizations
- Develop a normative culture in Luxembourg
  - Promotion
  - Education
  - Research



Luxembourg standardization strategy 2020-2030

Technical standardization

"Inclusive tool for performance and excellence to serve the economy"



→ Strategy signed by the Minister of the Economy of Luxembourg

PERFORMANCE

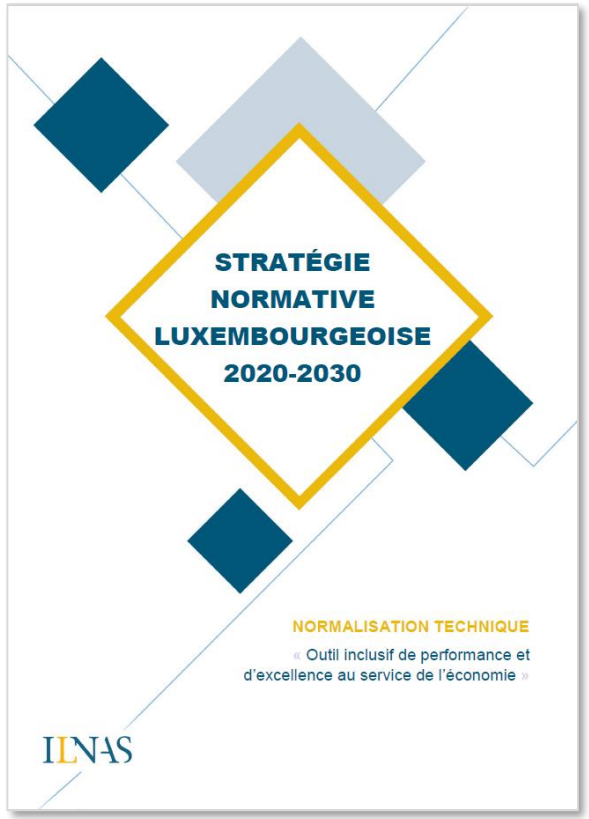
- ❑ **Pillar 1 – Use of relevant technical standards**
- ❑ **Pillar 2 – Involvement in the standardization process**

EXCELLENCE

- ❑ **Pillar 3 – Active participation of the NSB in the European and international standardization organizations**
- ❑ **Pillar 4 – Development of research and education about standardization**

https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

Luxembourg standardization strategy 2020-2030

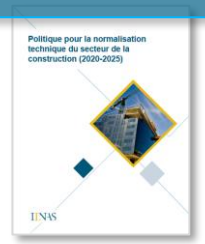


Technical standardization

"Inclusive tool for performance and excellence to serve the economy"

3 growth sectors identified

CONSTRUCTION



INFORMATION AND COMMUNICATION TECHNOLOGIES

AEROSPACE

Identification of trans-sectoral standardization interactions

- Computer Aided Design (CAD)
- Building Information Modelling (BIM)
- 3D printing
- …

- Space data processing
- Space traffic management
- Smart Mobility
- …

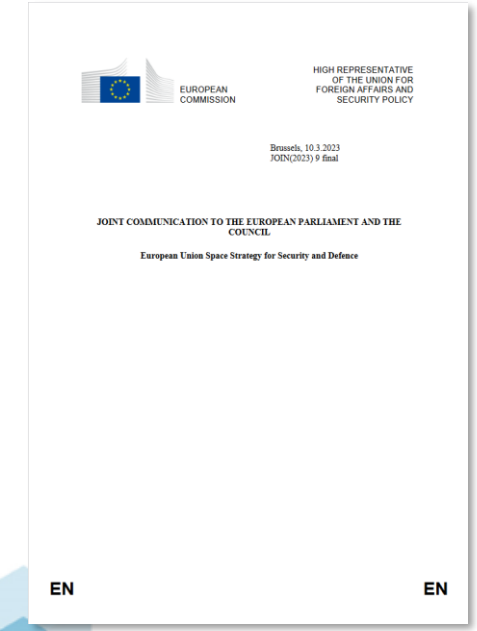
"Foster and strengthen the national involvement in standardization work"

1. Promoting technical standardization to the market
2. Reinforcing the valorization and the involvement in technical standardization
3. Supporting and strengthening the EaS and the related research activities

IV - Luxembourg standardization strategy 2020-2030 – Highlights

A need for standards and involvement of the market

- **Pillar 1 – Use of relevant technical standards**
- **Pillar 2 – Involvement in the standardization process**



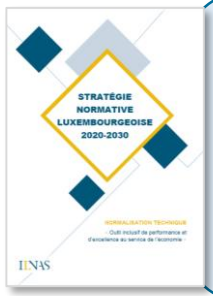
JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL "European Union Space Strategy for Security and Defence" (03.2023)

[…] the ***implementation of the NIS 2 Directive and the upcoming Cyber Resilience Act, as well as other existing cybersecurity frameworks, will incentivise the uptake of cybersecurity requirements for critical digital products that are used in space****. Specific cybersecurity standards and procedures in the space domain could be considered as part of the EU Space Law where relevant.*

Finally, ***greater steering of the EU in the development of standards and its better representation in international standardisation organisations are crucial, in particular to protect the security interests of the EU and its Member States****. Coherence with North Atlantic Treaty Organization (NATO) standards will be encouraged. […]*

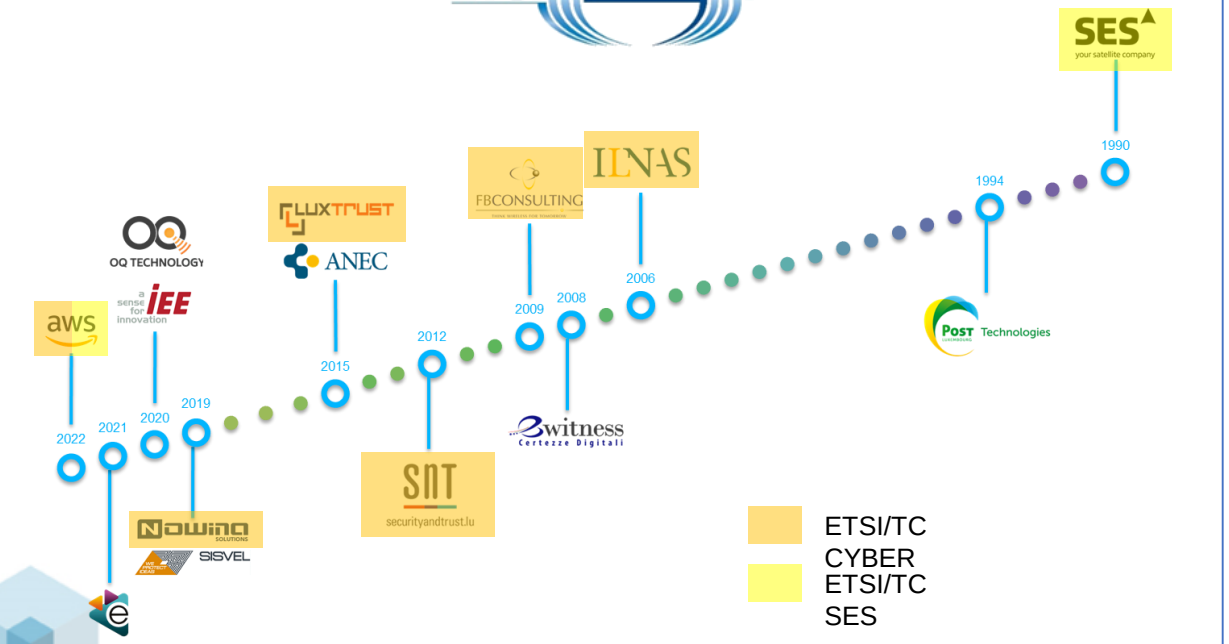
IV - Luxembourg standardization strategy 2020-2030 – Highlights

Current involvement of the national market in some relevant technical standardization activities

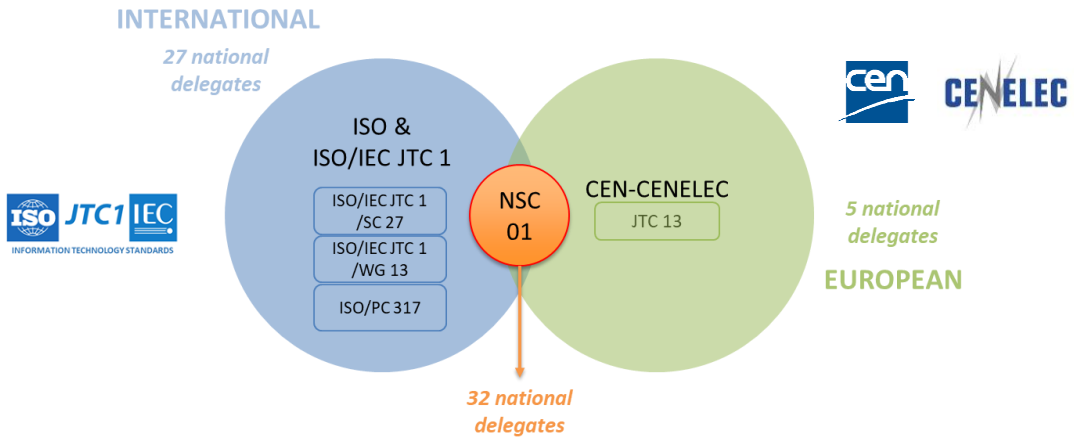


- **Pillar 1 – Use of relevant technical standards**
- **Pillar 2 – Involvement in the standardization process**

ETSI



National Standardization Commission "Cybersecurity"

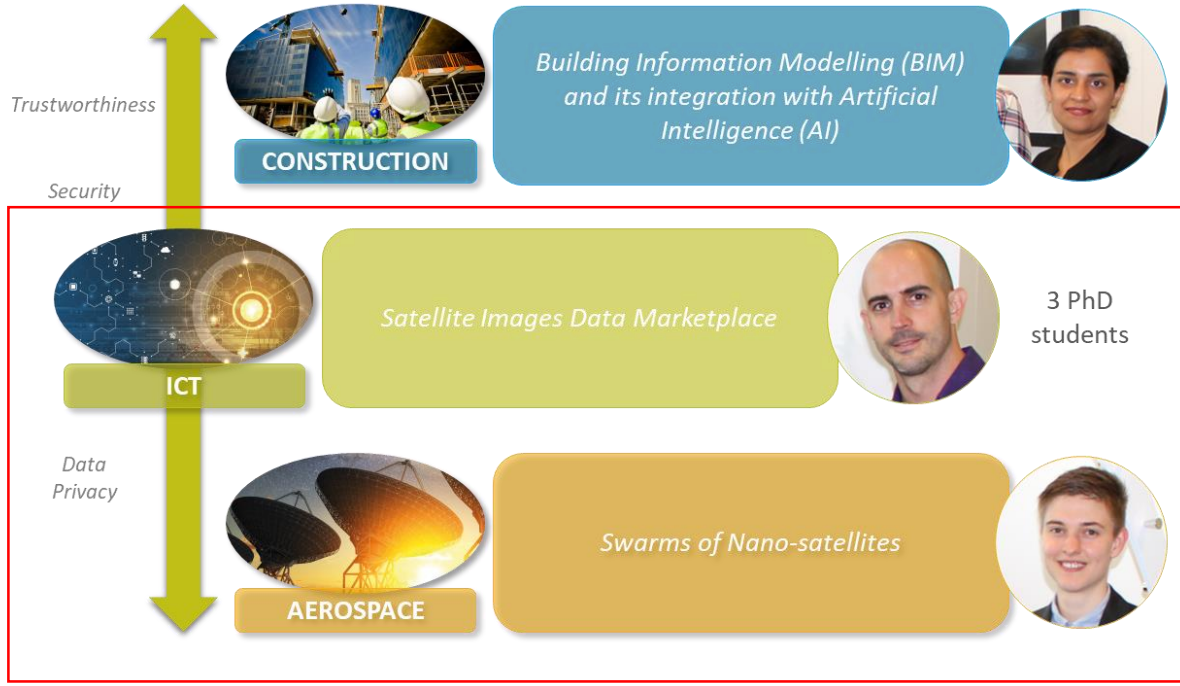


IV - Luxembourg standardization strategy 2020-2030 – Highlights

Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024)

- **Pillar 3 – Active participation of the NSB in the European and international standardization organizations**
- **Pillar 4 – Development of research and education about standardization**

Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024) in collaboration with the University of Luxembourg



IV - Luxembourg standardization strategy 2020-2030 – Highlights

Research project CORAL - cybersecurity Certification based On Risk evALuation and treatment

- **Pillar 3 – Active participation of the NSB in the European and international standardization organizations**
- **Pillar 4 – Development of research and education about standardization**

CORAL

CORAL - cybersecurity Certification based On Risk evALuation and treatment

Overview

CORAL is a European Union-funded project under CEF Telecom Call, that **aims to elaborate a toolkit and methodology to speed up the certification process in line with the EU Cybersecurity Act** or CSA (Regulation EU 2019/881). The project aims to address challenges concerning self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with the CSA.

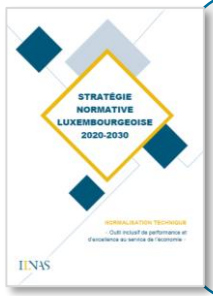
The CORAL project is being developed in a Luxembourgish context, but it aims to become known and used beyond the Luxembourg market and borders. Its target audience is primarily small and medium enterprises who have a product or service for which, they wish to assess the basic cybersecurity requirements.

Co-financed by the Connecting Europe Facility of the European Union

CORAL website: https://coral-project.org/ Fit4CSA tool: https://fit4csa.nc3.lu/

IV - Luxembourg standardization strategy 2020-2030 – Highlights

Master program (MTECH)



- **Pillar 3 – Active participation of the NSB in the European and international standardization organizations**
- **Pillar 4 – Development of research and education about standardization**

Master in Technopreneurship (MTECH)

Master MTECH (2023-2024) – ILNAS in collaboration with the University of Luxembourg and the Chamber of Employees

PROGRAMME

STANDARDISATION	ECTS
Smart Secure ICT and Innovation	1
Technical Standardisation	3
TOTAL	4

SMART ICT	ECTS
Smart ICT Technologies I	5
Smart ICT Technologies II	5
TOTAL	10

DIGITAL TRUST FOR SMART ICT	ECTS
Security for Smart ICT I	2
Security for Smart ICT II	3
Trust Architectures for Smart ICT	4
TOTAL	9

TECHNOPRENEURSHIP	ECTS
Management of Business and Technical Innovation	3
Digital Intelligence	2
Legal Aspects	2
TOTAL	7

MASTER THESIS	ECTS
Master Thesis	30
TOTAL	30

332 hours of teaching

60 ECTS

Internship (+/- 750 hours)

Started in February 2023

2 years lifelong-learning

11 Modules

9 students

With the support of: THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy

CEN CENELEC ETSI

Thank you for your attention!

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail: info@ilnas.etat.lu
www.portail-qualite.lu

Words of the Ministry of the Economy

Mr. François THILL
Cyber Security Director
Ministry of the Economy

(Security) Standards and Challenges

François Thill, Director cybersecurity and digital technologies,

Ministry of the Economy

LUXEMBOURG
TRADE & INVEST

Importance of Security Standardization

- The role of management processes in security standards
- ISO 27005 as an example of risk management

Individual Effort and Subjectivity

- Need for additional individual effort in implementing security standards
- Individualistic approaches can lead to subjective decisions and flawed results
- Won’t lead to comparability with peers for the sake of governance and continuous improvement

Market Failures in Cybersecurity

- What are market failures?

Markets fail when the market (based on private actors) does not provide a good or service even though the economic benefits outweigh the economic costs(*).

(*)European State Aid Control: An Economic Framework, Hans W. Friederiszick, Lars-Hendrik Röller, and Vincent Verouden, page 633, accessed on 08/05/2023 at https://ec.europa.eu/dgs/competition/economist/esac.pdf

Market Failure: Coordination Failure

- Lack of common practices and interoperability among cybersecurity providers

Market Failure: Asymmetry of Information

- SMEs are unaware of cybersecurity exposure and lack information about current threats and effective security measures

Market Failure: Lack of Incentives

- Absence of understanding incentives for sharing threat information

Market Failure: Absence of Supply

- Lack of "unattended" or "fully automatic" cybersecurity tools for decentralized data processing architectures, particularly affecting SMEs

Impact of Market Failures

- 80% of companies are poorly protected due to market failures with devastating impacts on supply chains

Collaboration Initiatives in Luxembourg

- Importance of intense operative collaboration and continuous sharing of threat intelligence
- Creation of open source collaborative cybersecurity tools and an open cybersecurity data space

Data-Driven Cybersecurity

- Data is crucial for operating cybersecurity and for developing unattended tools for SMEs

Call for Collaboration in the Space Sector

- Intensify operational collaboration in the space sector, particularly in cybersecurity
- Establishment of a space Incident Response Team and sectorial threat intelligence sharing

Thank you!

tradeandinvest.lu

LuxTradeInvest

www.linkedin.com/company/luxembourg-trade-and-invest/

www.youtube.com/c/LuxembourgTradeandInvest

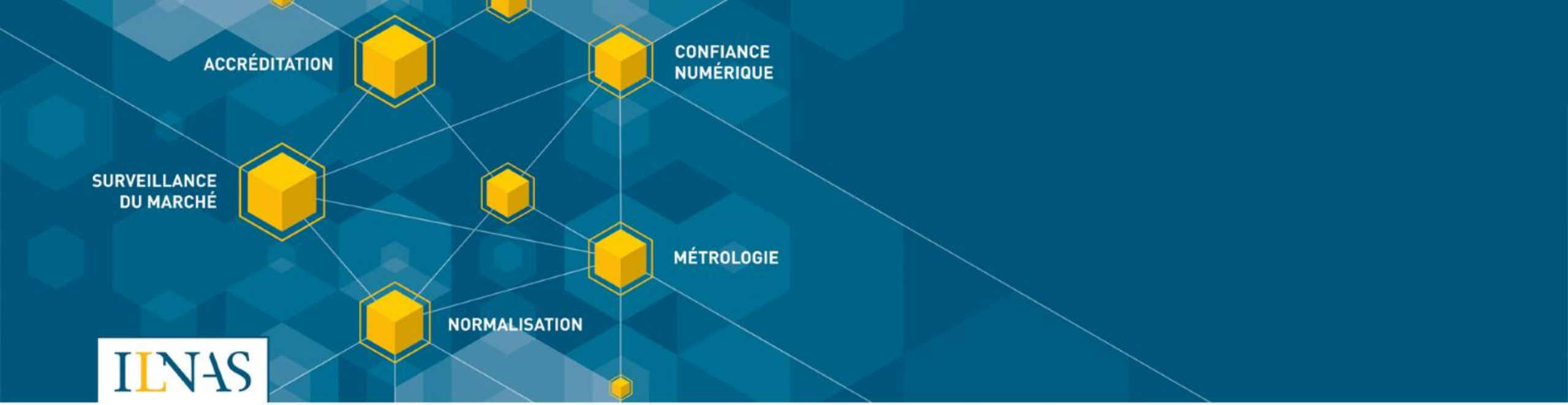
François Thill

Director cybersecurity and digital technologies

LUXEMBOURG
TRADE & INVEST

National Standardization Policy for the Space Sector

Mr. Jérôme HOEROLD
Head of department - ILNAS/OLN



Workshop – Technical Standardization in Space and Cybersecurity

National Standardization Policy for the Space Sector

27th June 2023

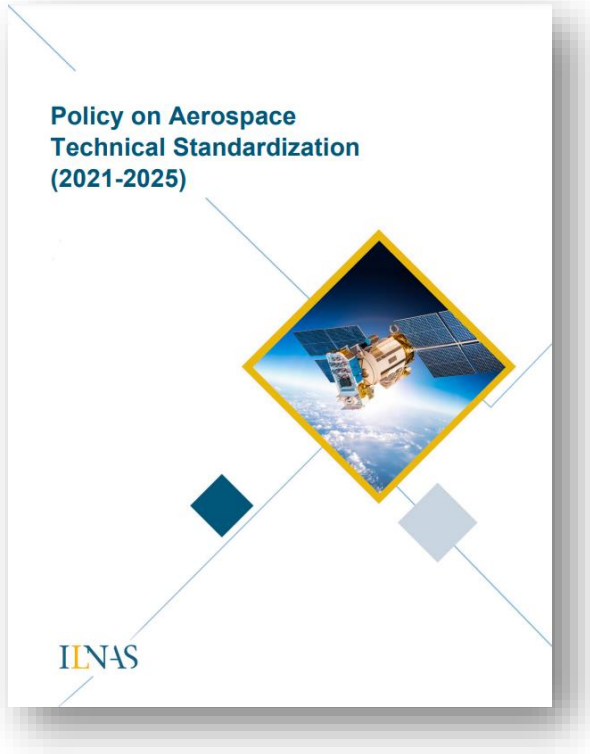
Jérôme HOEROLD – Head of Department, ILNAS/OLN

I – Policy on Aerospace Technical Standardization

Introduction

- In January 2021, ILNAS published its « Policy on Aerospace Technical Standardization (2021 - 2025) ».
- The objective of this policy is to promote and strengthen the involvement of the national market in standardization activities through three flagship projects:

  - **Promoting aerospace technical standardization to the market**
  - **Reinforcing the valorization and the involvement regarding aerospace technical standardization**
  - **Supporting and strengthening Education about Standardization and the related research activities**

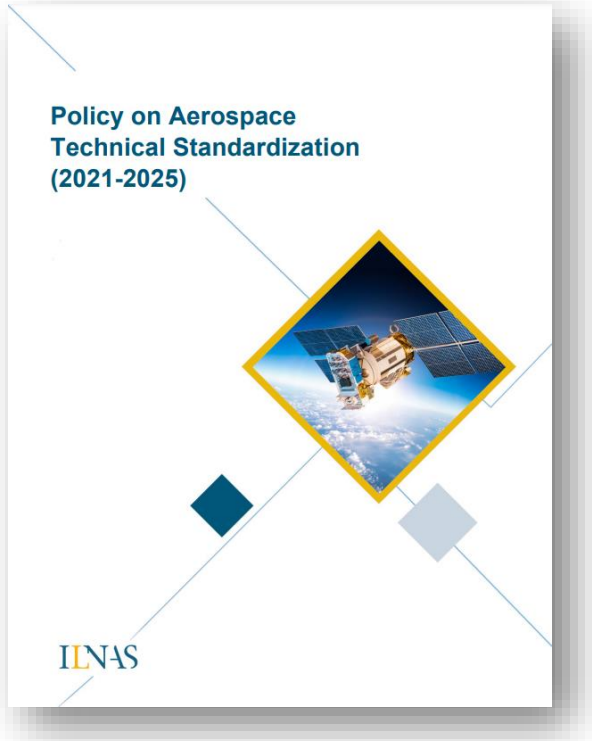


A. Draw up a yearly national standards analysis for the aerospace sector

→ **Sector-based "Snapshot"**

This document is composed of different type of information:

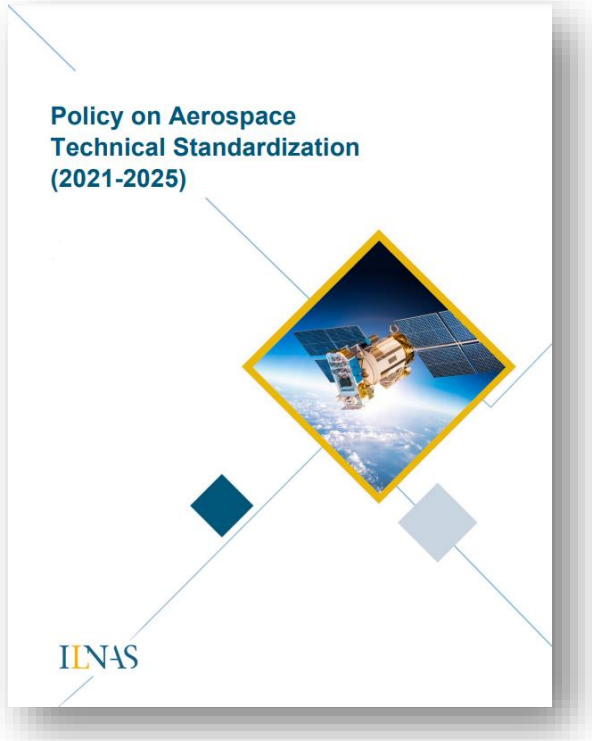
- **Standards watch of the related sector**
  - Inventory of standards – both published and under development – at the European and international levels
  - Identification and description of technical standardization committees
  - Mention of the related national representation
- **Relevant national companies, agencies and Fora/Consortia related to the aerospace sector**
- **Final report with the results of the above mentioned standards watch and the identified opportunities**



B. Define a national implementation plan for aerospace technical standardization

The aim is **to involve targeted stakeholders of the Grand Duchy of Luxembourg in a global approach to standardization in order to support the sector in terms of competitiveness, visibility and performance, while enhancing the international recognition of Luxembourg at the standards level**

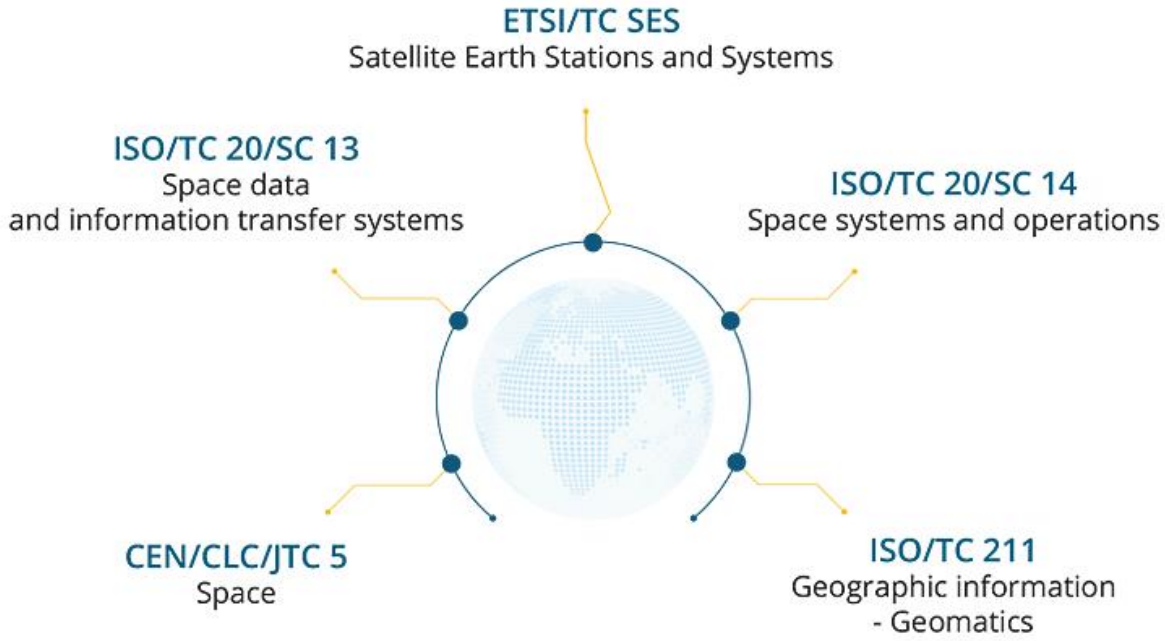
The implementation plan is drawn up on a yearly basis in order to ensure that it is in line with the national standardization priorities



A. Participate in relevant technical committees

In order to provide the most relevant information on technical standardization to the national aerospace community, ILNAS analyzed the national market needs of this specific sector in order to define a list of relevant technical committees.

These technical committees are followed by ILNAS in order to provide the most relevant information to the interested national actors.



B. Promote the participation of the national market in technical standardization committees and the use of relevant standards

Three main actions have been defined:

1) Promote the use of the ILNAS reading stations

- Free consultation of European (CEN, CENELEC & ETSI), international (ISO & IEC) and national (ILNAS & DIN) standards
- More than 200.000 normative documents at your disposal
- National network currently composed of 9 lecture stations

2. Reinforcing the valorization and the involvement regarding Aerospace technical standardization

2) *Organize events to promote participation in technical standardization committees and the use of relevant standards in the aerospace sector*

Workshop Space and Technical Standardization and Presentation of the new ANS Aerospace (June 2022)

Online training – Aerospace standardization (July 2021)

Presentation of ISO 24113 – Space debris mitigation (November 2021)

3) *Meet and raise the awareness of the national stakeholders (companies, national agencies, Fora/Consortia, etc.) of the aerospace sector*

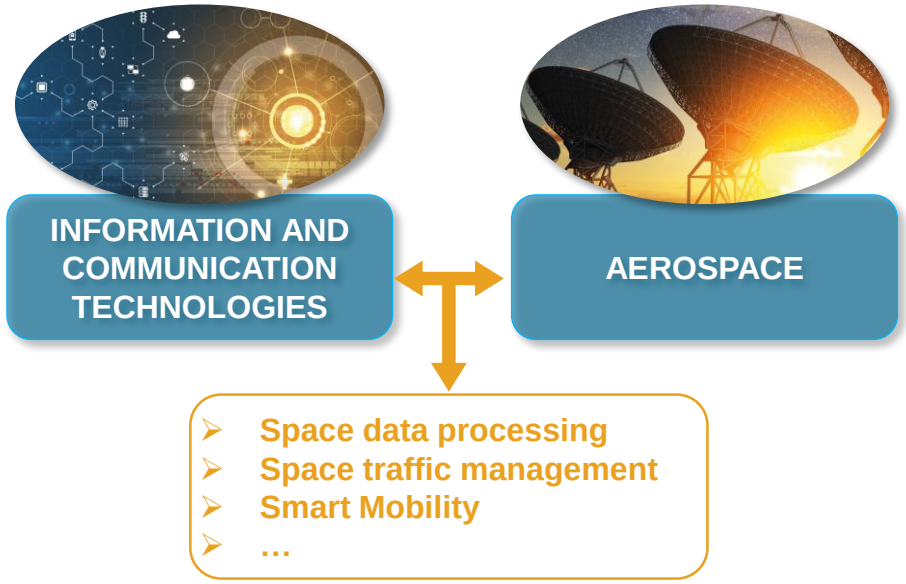
C. Create transversal links with the ICT domain

The aerospace sector is evolving in parallel with the development and the usage of ICT.

→ **It is important to create transversal links with technical standardization of the ICT domain in order to identify new opportunities for common developments.**

Relevant information will be provided to the national stakeholders active in the aerospace sector, in order to allow them :

- to improve the efficiency of their processes
- to facilitate communication
- to identify new business opportunities
- to develop new markets



3. Supporting and strengthening education about standardization and the related research activities

ILNAS is constantly **reinforcing the research and innovation activities related to technical standardization in the aerospace sector**, notably by defining and carrying out new research and education projects.

In this frame, the developments are/could be:

- Analysis of the current research trends and outlooks related to the aerospace sector
- Support of doctoral students (in collaboration with the University of Luxembourg), for example on research projects concerning the use of ICT in the aerospace sector
- The publication of white papers and / or other research publications on technical standardization in the field of aerospace
- Evaluate the possibilities to integrate educational content on aerospace technical standardization into educational programs or creating new educational programs dedicated to aerospace technical standardization

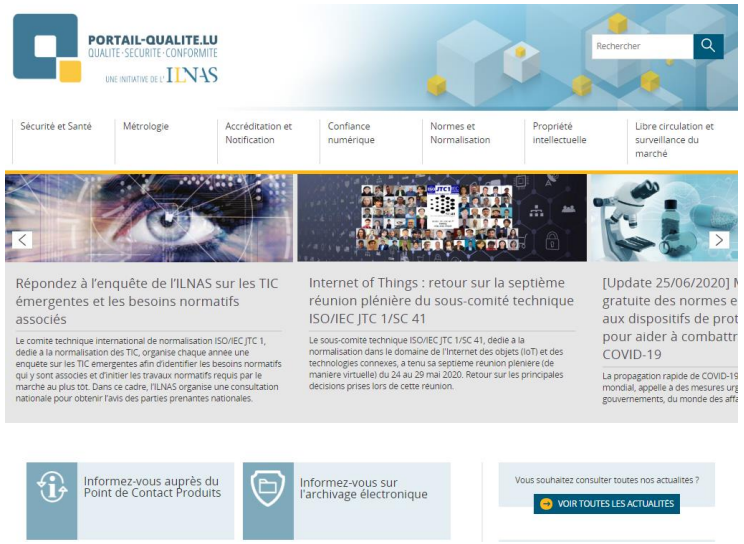
Conclusion

The Luxembourg's policy on aerospace technical standardization (2021-2025) will enable to:

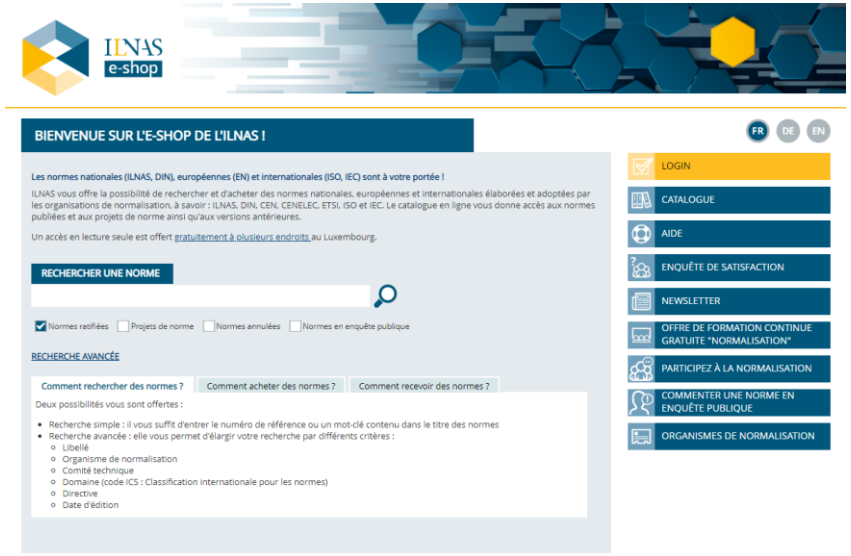
- Strengthen the national aerospace standardization community
- Organize and develop the aerospace technical standardization community at national level
- Raise awareness on aerospace technical standardization according to the market needs
- Increase the national representation within European and international technical committees in the field of aerospace technical standardization
- Foster the use of relevant standards in business activities for the benefit of the national stakeholders
- Develop research and education activities in relation to aerospace technical standardization considered as being of national interest

For more information

Portail qualité
www.portail-qualite.lu



ILNAS e-shop
ilnas.services-publics.lu



Organisme luxembourgeois de normalisation

Tel. : (+352) 247 743 40
Fax : (+352) 247 943 40
E-mail : normalisation@ilnas.etat.lu

Thank you for your attention!

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail: info@ilnas.etat.lu
www.portail-qualite.lu

The challenges for cybersecurity and space
An ESA Security Engineer perspective

Mr. John Charles IRVING
Security Engineering Manager – ESA

ESA & Cyber Security – how is ESA addressing the dynamic world of Security & Space

John Irving

ESA Security Office

2023

V1.4

AGENDA

1. Context & History Of Attacks for Security & Space
2.
3.
4.
5.

Some history of attacks (Industrial Control Systems)

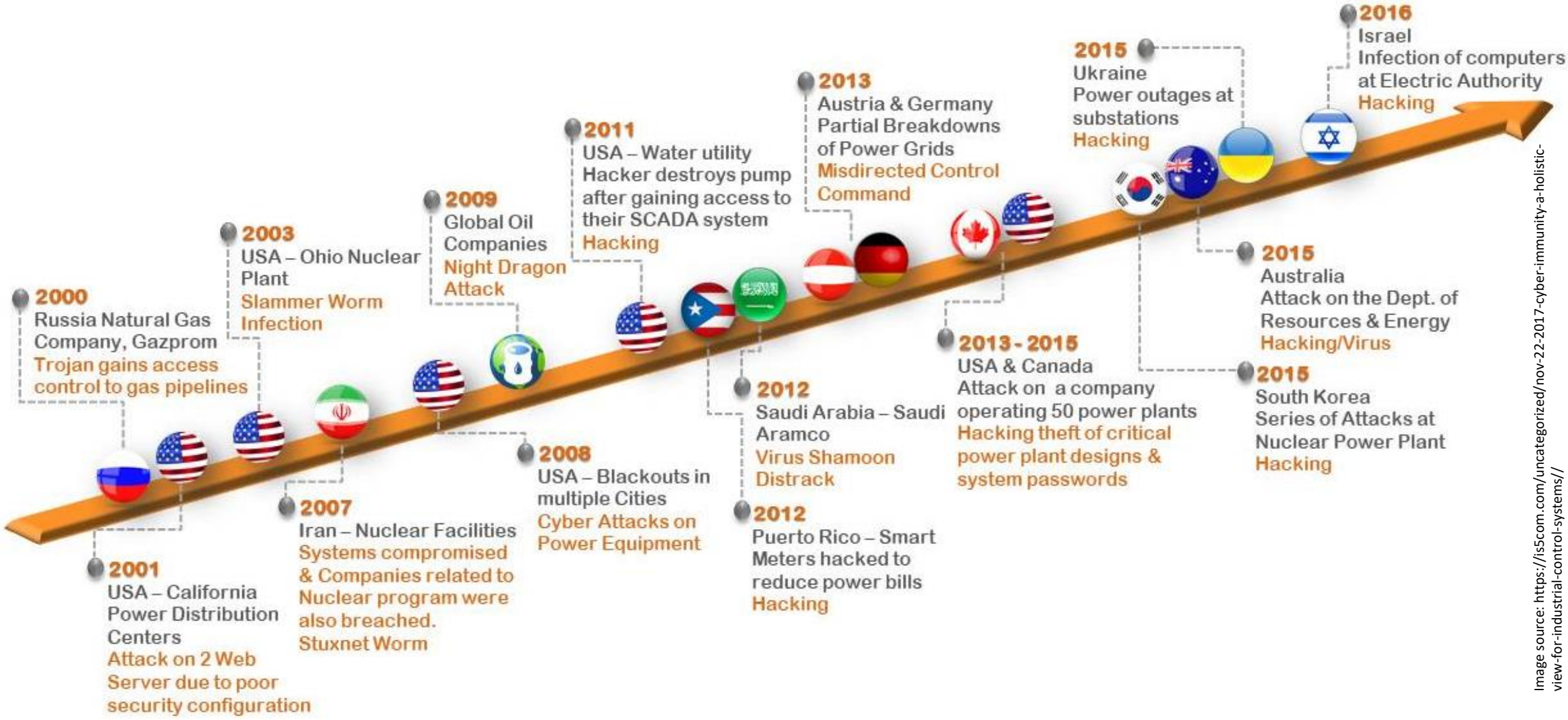


Image source: https://is5com.com/uncategorized/nov-22-2017-cyber-immunity-a-holistic-view-for-industrial-control-systems//

Example of Space Industry Related Attacks (publicly available) 1998 - 2014

2014

NOAA Satellite hacked causing weather service disruption
2010/2011 NASA declare 5,408 incidents – JPL compromise including unencrypted laptop with ISS control codes

2008

Johnson space centre infected with malware,
uplink disrupted to ISS due to old on-board o/s
Ground Station hacked controlling scientific satellite

2007

Norway G-Station used to "interfere' with two satellites
4 times in 2 years

2006

Satellite Jamming in Israel-Lebanon War
2005 NASA KSC vehicle & assembly data exfiltration

1998

2000 15 year old jailed after 21 day shutdown of NASA computers
1999 **US-German ROSAT X-ray satellite taken over, rendered useless**,crash 2011
1999 UK SkyNet Ransom

Image: Irving

Example of Space Industry Related Attacks (publicly available) 2015 - 2021

2022

ViaSat Terminals destroyed by space/cyber Attack
Thales Gemalto targeted attacking internal systems globally
NASA disconnect partners after SolarWinds Threat
Academic intercepts satellite data
2020 Plans of Boeing, Lockheed Martin equipment leaked online

2021

IRGC Backed group infiltrates US & IR satellite companies (inc sat control computers)
Airbus attacked via supplier VPNs
Airbus Suppliers attacked
NASA Hacked due to unauthorized Shadow IT
Employee cryptomining using NASA networks
2018 external account hacked – 500Mbyte mission data

2019

2017

Leonardo (Italy) insider attack losing sensitive data
China intercept satellite video chat message (5 minutes)
NASA Goddard & JPL inc PII over 12 year period

2015

Turla APT satellite DVB-S link hijack

Image: Irving

Cyber-Security threats for Space Systems - examples

Gary Mckinnon - 2002

WIRED STAFF BUSINESS JUN 21, 2006 12:00 PM

'UFO Hacker' Tells What He Found

The search for proof of the existence of UFOs landed Gary McKinnon in a world of trouble. After allegedly hacking into NASA websites — where he says he found images of what looked like extraterrestrial spaceships — the 40-year-old Briton faces extradition to the United States from his North London home. If convicted, McKinnon could [...]

https://www.wired.com/2006/06/ufo-hacker-tells-what-he-found/

https://pixabay.com/de/photos/ufo-entf%C3%BChrung-fantasie-6073925/

McKinnon, whose lawyers describe him as a "UFO eccentric" who used the Internet to search for alien life, is accused of causing the U.S. Army's entire network of more than 2,000 computers in Washington to be shut down for 24 hours. U.S. authorities called this "the biggest military hack of all time".

https://www.reuters.com/article/idINIndia-43041020091009

Example – Viasat attack

- Viasat communications company with over 2$ Billion per annum
- Full suite of services (ground antenna, mobile, communications, GSAAS, design .. Production (modems, ASICs, Antenna, ISL…))

- Feb 24 2020 viasat is attacked.
- Mid March 2020 viasat reported an attack on European customers on is KA-SAT network operated by Eutelsat subsidiary Skylogic.

- Hacked via a misconfigured VPN device on the management network that did not have sufficient protection & monitoring.
- Allowed a user modem update causing them to be configured in a way to make unusable.
- Still under investigation, US & UK attribute to Russia

Example of Space Attacks (GNSS Jamming/Spoofing)

Sabotage in UAE waters could lead to cyber attacks, former military officer says

Itai Sela, Naval Dome CEO, being a former senior officer in the military, commented on the attacks that took place in UAE's territorial waters, near the bunkering port of Fujairah. The attack concerns four vessels that were sabotaged in the Gulf of Oman, on May 12.

CYBER SECURITY | 15/05/19

Specifically, Mr Sela commented

> *While we hope these incidents will not escalate, shipowners with operations in the area must be vigilant and carry out inspections of all their PC-based navigation and machinery control systems. Ship operators should not allow crew members or technicians to plug-in USBs or external devices onboard or download maps and charts for specific areas, unless they absolutely need to do so.*

He also advised that operators check their insurance policies to ensure that OT systems are covered in the event of any cyber damage.

Need convincing? In 2013, a couple college students were able to take control of an $80 million, 213-ft luxury yacht using GPS spoofing, in which hackers send counterfeit location signals to throw off the system's autopilot. In case you think it's an isolated incident, they did the same thing to a drone.

Now imagine being trapped inside that malfunctioning computer program – at high speed. That's exactly what happened to a writer for Wired magazine when his Jeep was remotely hacked on the freeway.

ANDY GREENBERG SECURITY 07.21.2015 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Curious hackers inject ghost airplanes into radar, track celebrities' flights

What happens when a hacker gets bored and curious about airplane tracking systems? In the case of Brad "RenderMan" Haines, aka @ihackedwhat, a very interesting Def Con 20 presentation happened called "Hacker + Airplanes = No Good Can Come Of This."

French are accused of tank trials sabotage

FRENCH secret agents have been accused of trying to sabotage the North-East's billion pound bid to supply the Greek government with Challenger 2 tanks.

The contract for the 60 tonne tanks, made at Vickers Defence Systems, at Scotswood, beside the River Tyne in Newcastle, is believed to be worth up to £2.4bn.

Vickers faces competition from France, Germany and America - but it is the French who have been accused of spoiling the trials of their rivals.

During tests in Greece, several British and American tanks suffered navigation problems, and a military source revealed that jamming equipment was interfering with a high-tech satellite global positioning system.

https://youtu.be/ctw9ECgJ8L0

Good guys turned bad… or just did it wrong …

Police arrest two in data theft cyberattack on Leonardo defense corp

By **Lawrence Abrams** December 5, 2020 03:33 PM

The July Galileo Outage: What happened and why

Nov 07 2019 *10 mins read*

Accident details

It is indeed true that a presentation was held in Florida where details were shared with that audience, and by paying $24 we can download the presentation that was held there. From the slides, we learn that the outage stemmed from a failure in the system that determines the satellite orbits and clock parameters, which are normally uploaded to the satellites many times per day.

The outage in the ephemeris provisioning happened because simultaneously:

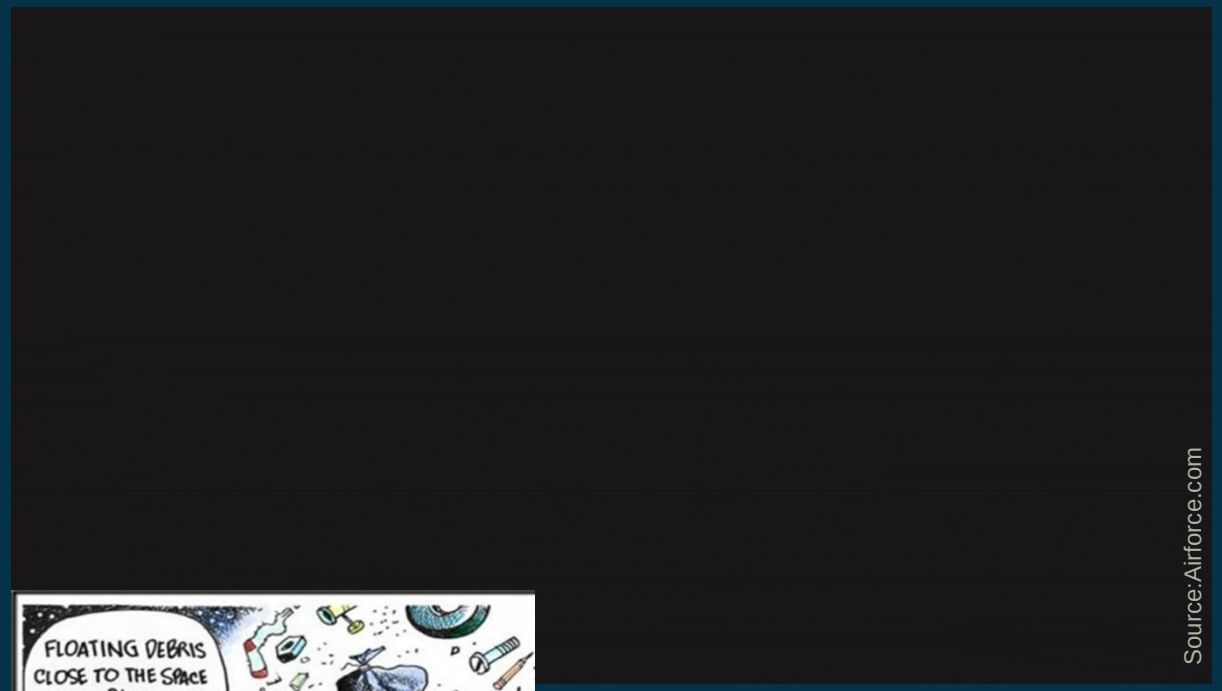
- The backup system was not available
- New equipment was being deployed and mishandled during an upgrade exercise
- There was an anomaly in the Galileo system reference time system
- Which was then also in a non-normal configuration

ESA under constant probing

- “*BECAUSE XMAS IS COMING AND WE HAD TO DO SOMETHING FOR FUN SO WE DID IT FOR THE LULZ.*”

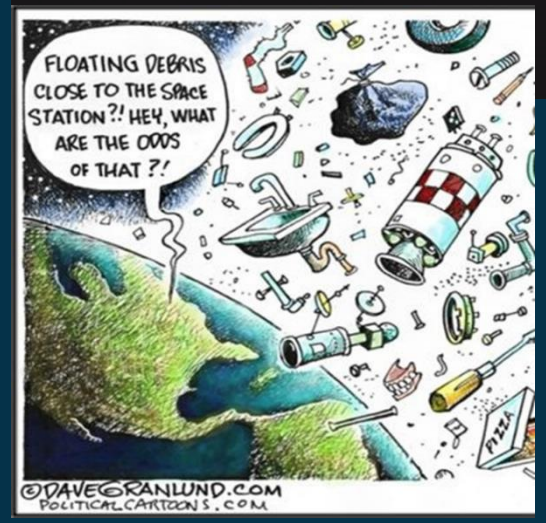
https://fossbytes.com/anonymous-hacks-european-space-agency-just-for-the-lulz/

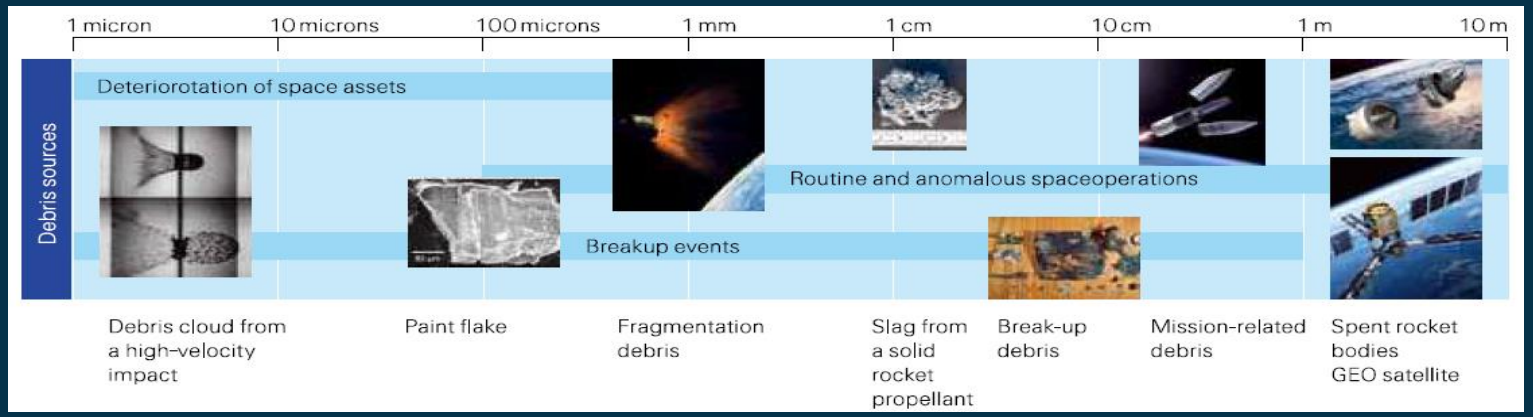
Environmental and Counterspace Threats - Space is Dangerous



Source:Airforce.com

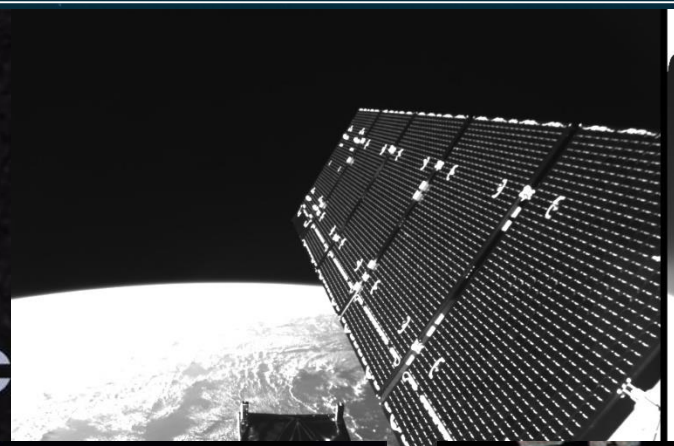
Souce: SpaceX, Dophinfan201

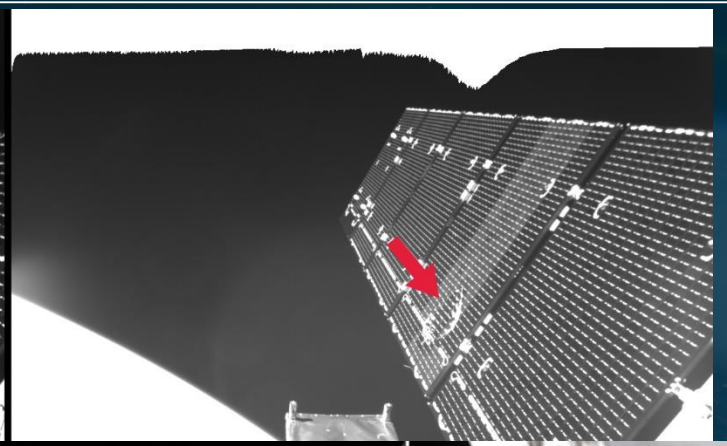


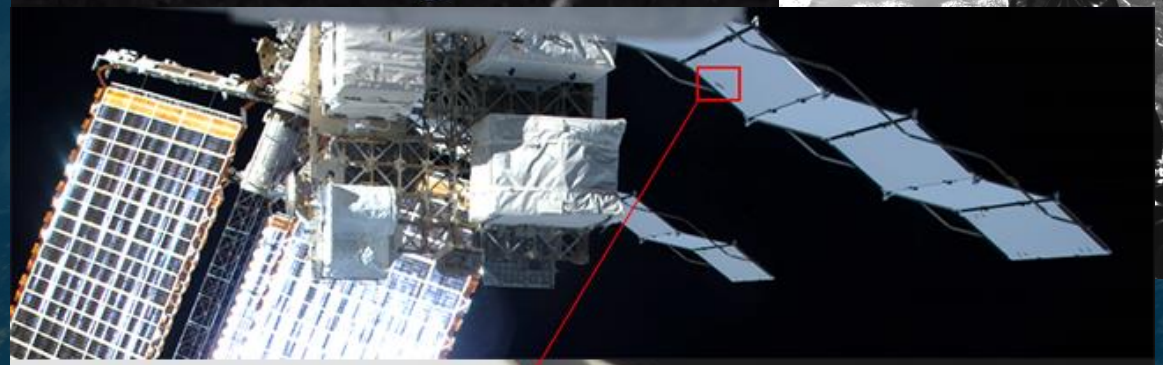


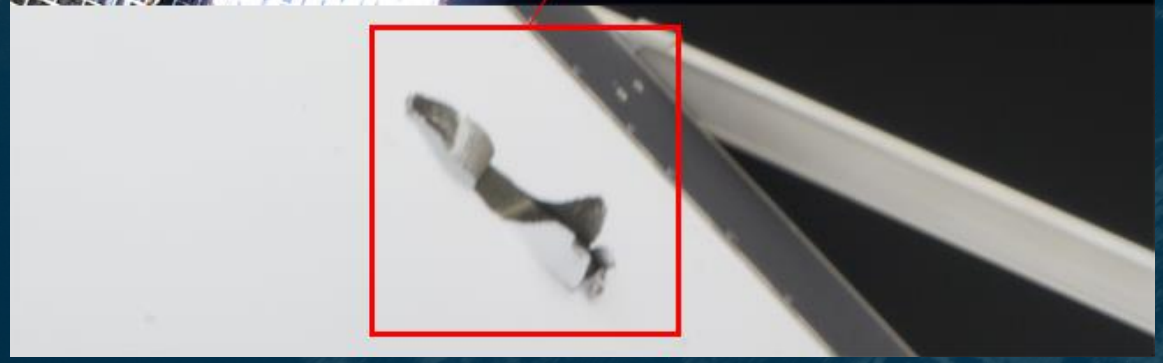
Souce: SwissRe

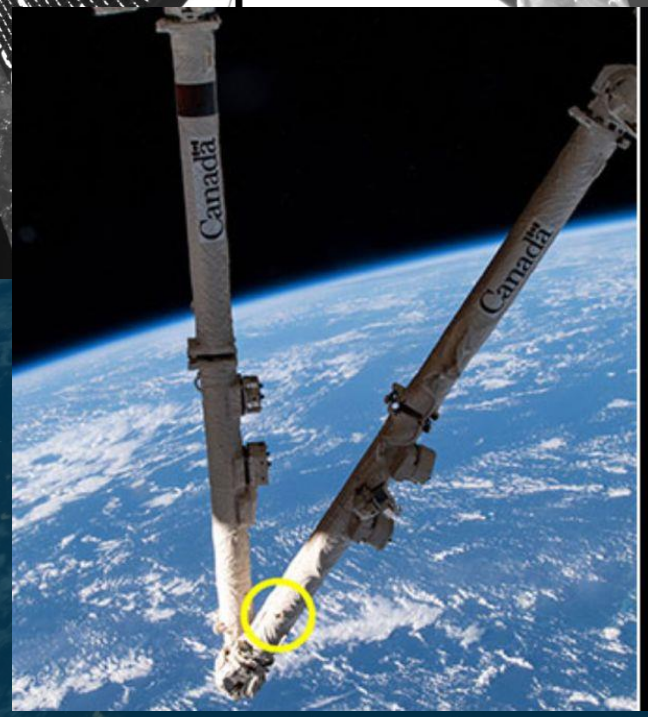
Environmental Threats in Space



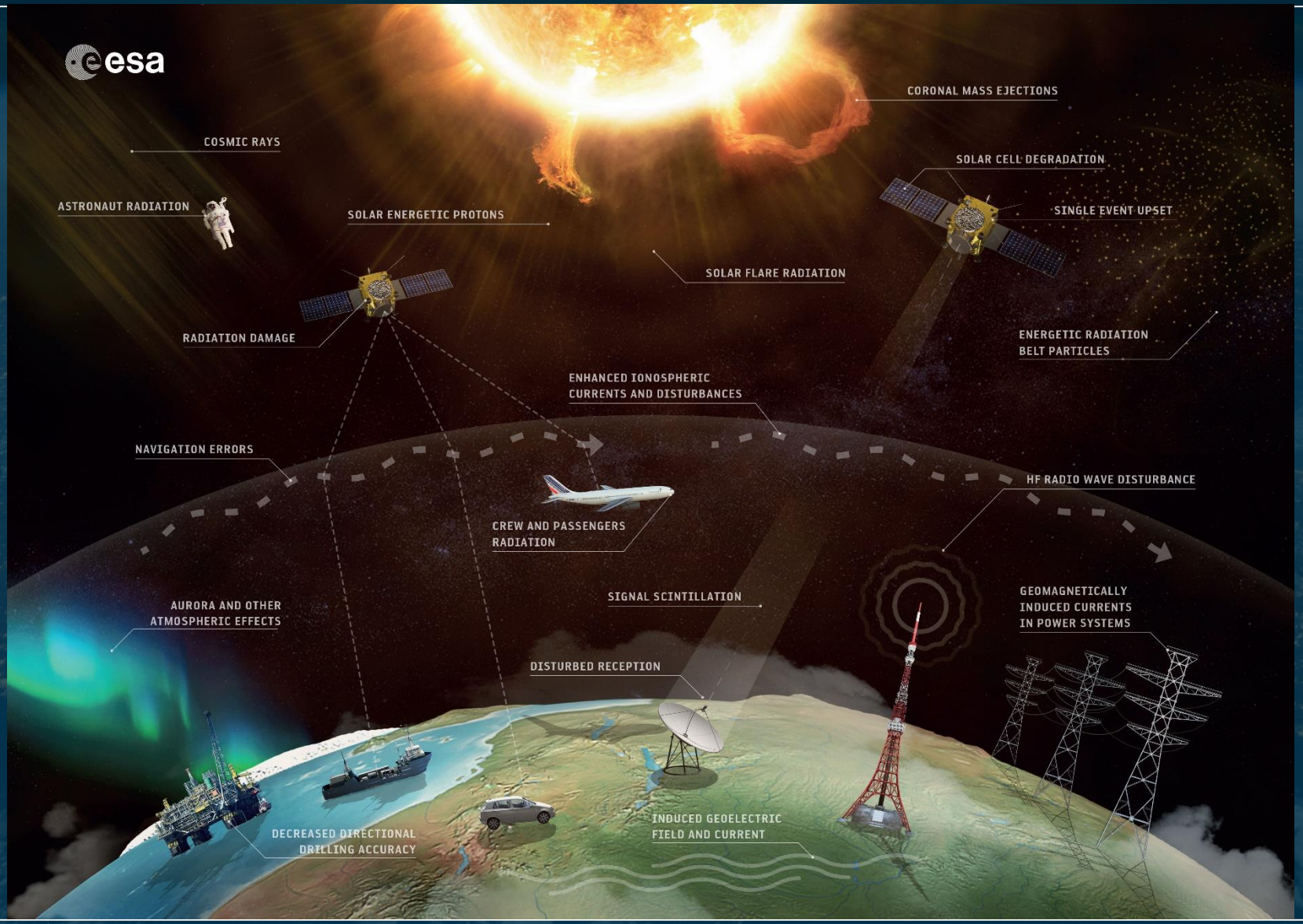


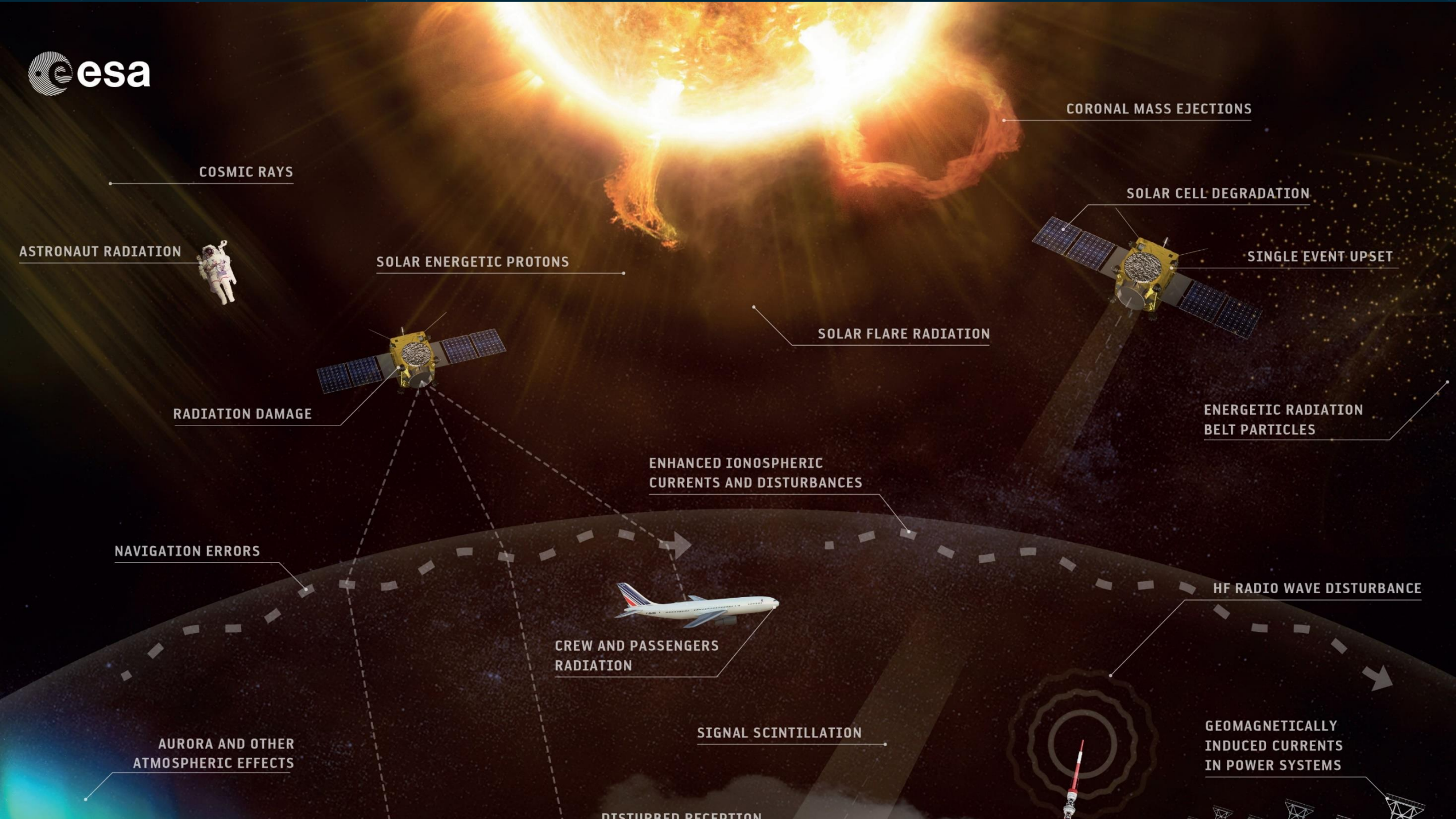


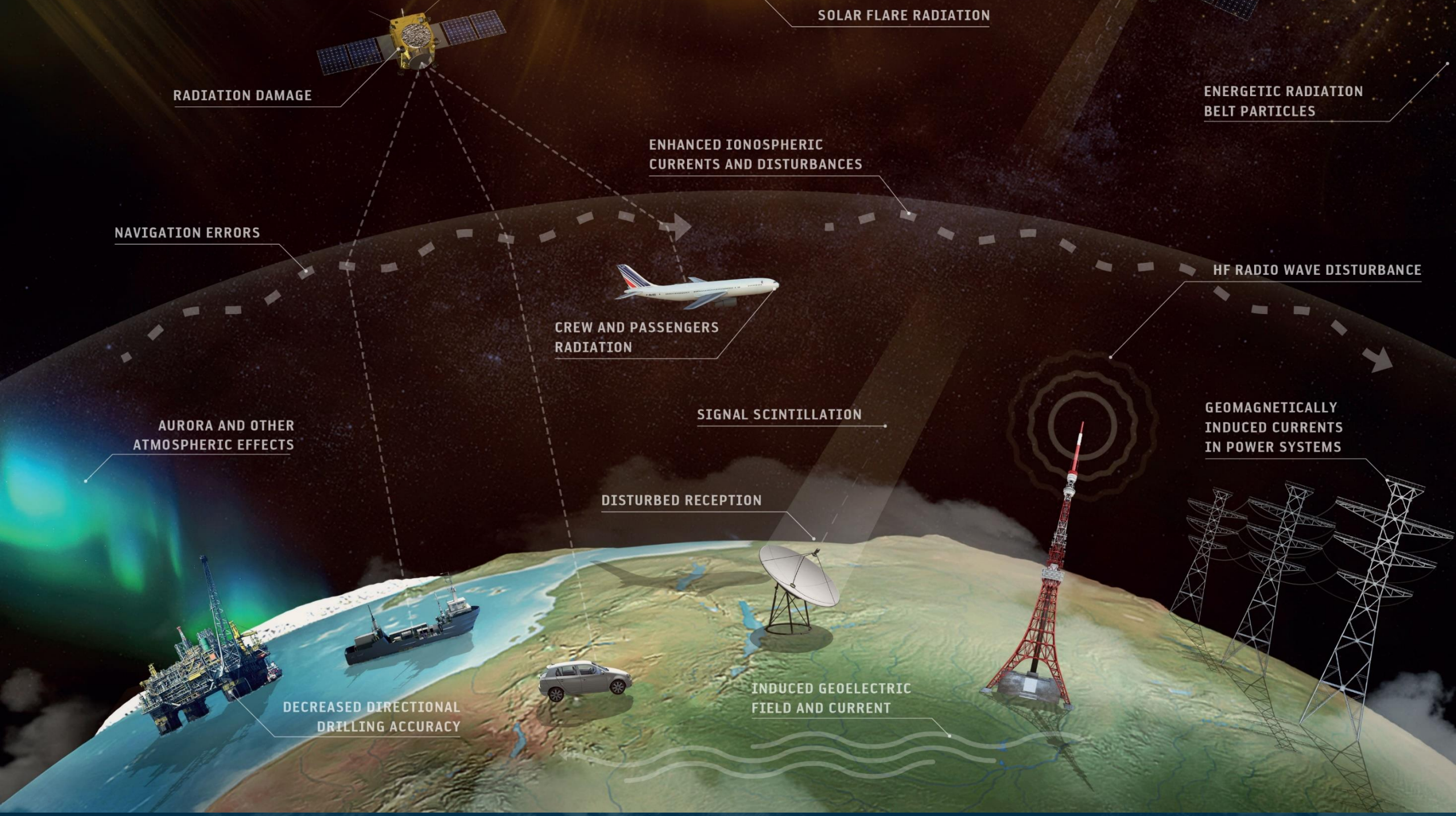




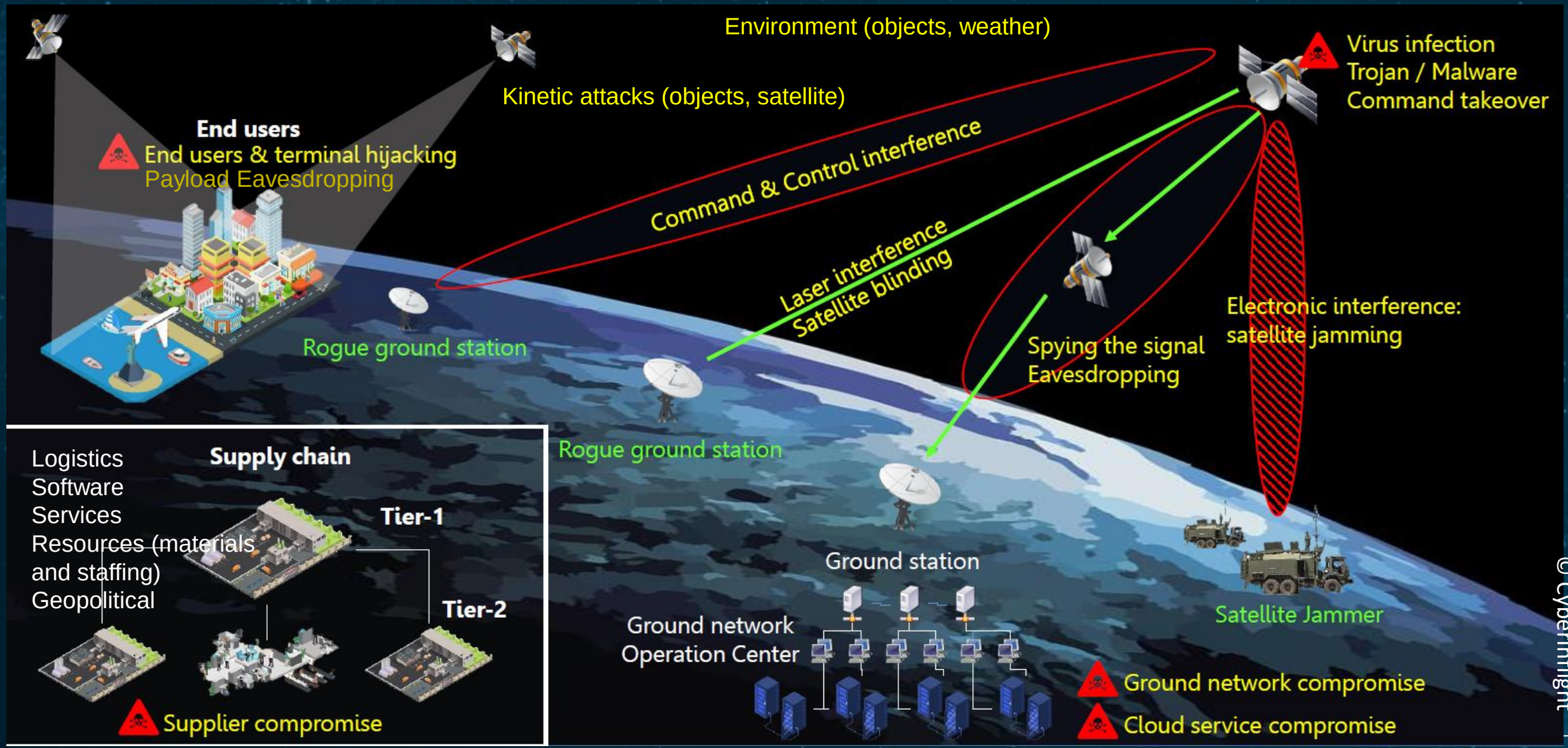
Space Weather Environment




esa
CORONAL MASS EJECTIONS
COSMIC RAYS
SOLAR CELL DEGRADATION
ASTRONAUT RADIATION
SINGLE EVENT UPSET
SOLAR ENERGETIC PROTONS
SOLAR FLARE RADIATION
RADIATION DAMAGE
ENERGETIC RADIATION
BELT PARTICLES
ENHANCED IONOSPHERIC
CURRENTS AND DISTURBANCES
NAVIGATION ERRORS
HF RADIO WAVE DISTURBANCE
CREW AND PASSENGERS
RADIATION
SIGNAL SCINTILLATION
AURORA AND OTHER
ATMOSPHERIC EFFECTS
GEOMAGNETICALLY
INDUCED CURRENTS
IN POWER SYSTEMS
DISTURBED RECEPTION


SOLAR FLARE RADIATION
RADIATION DAMAGE
ENERGETIC RADIATION
BELT PARTICLES
ENHANCED IONOSPHERIC
CURRENTS AND DISTURBANCES
NAVIGATION ERRORS
HF RADIO WAVE DISTURBANCE
CREW AND PASSENGERS
RADIATION
AURORA AND OTHER
ATMOSPHERIC EFFECTS
SIGNAL SCINTILLATION
GEOMAGNETICALLY
INDUCED CURRENTS
IN POWER SYSTEMS
DISTURBED RECEPTION
DECREASED DIRECTIONAL
DRILLING ACCURACY
INDUCED GEOELECTRIC
FIELD AND CURRENT

Intentional Threats to the Space Ecosystem



Impacts from Space Threats (Counterspace)

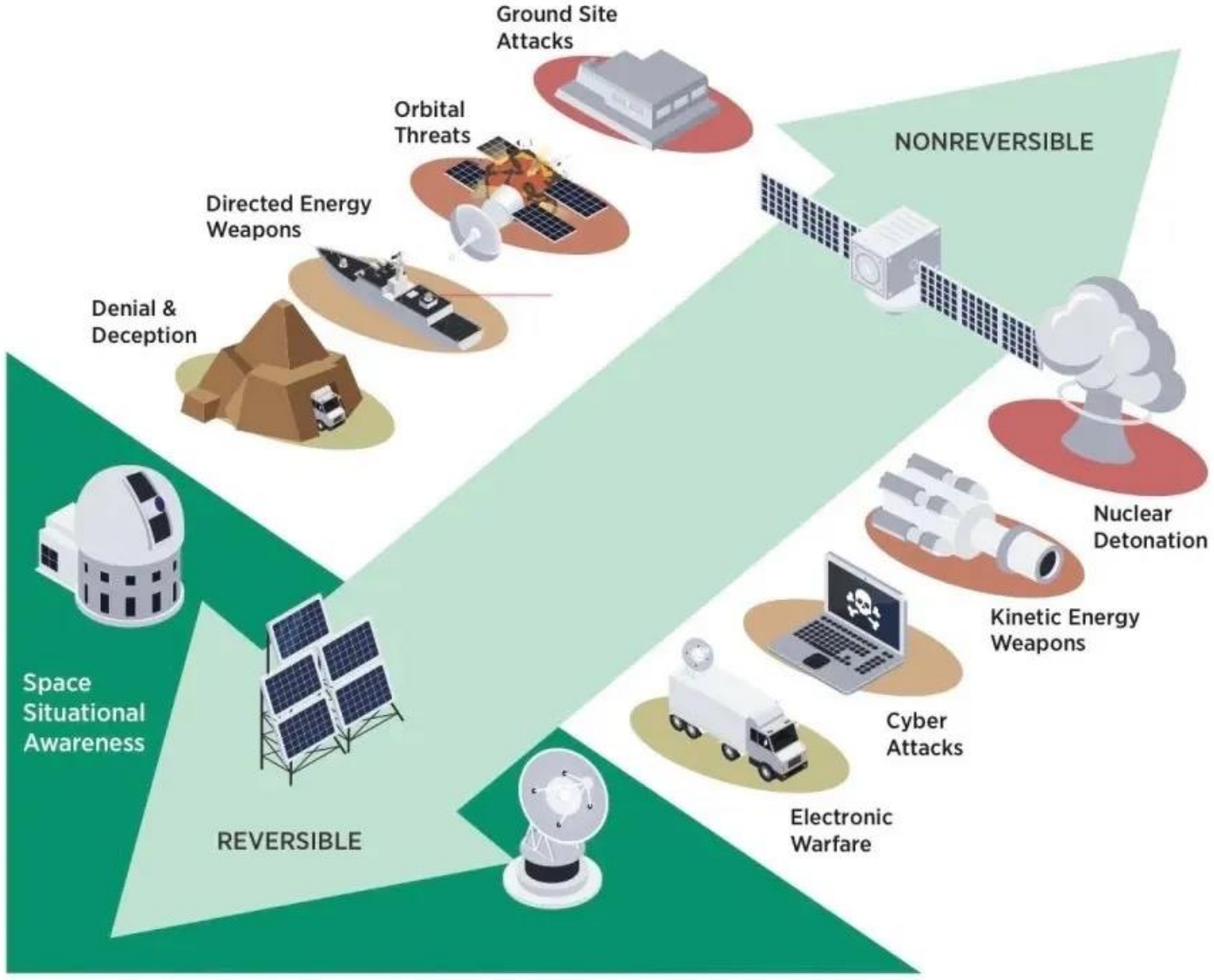
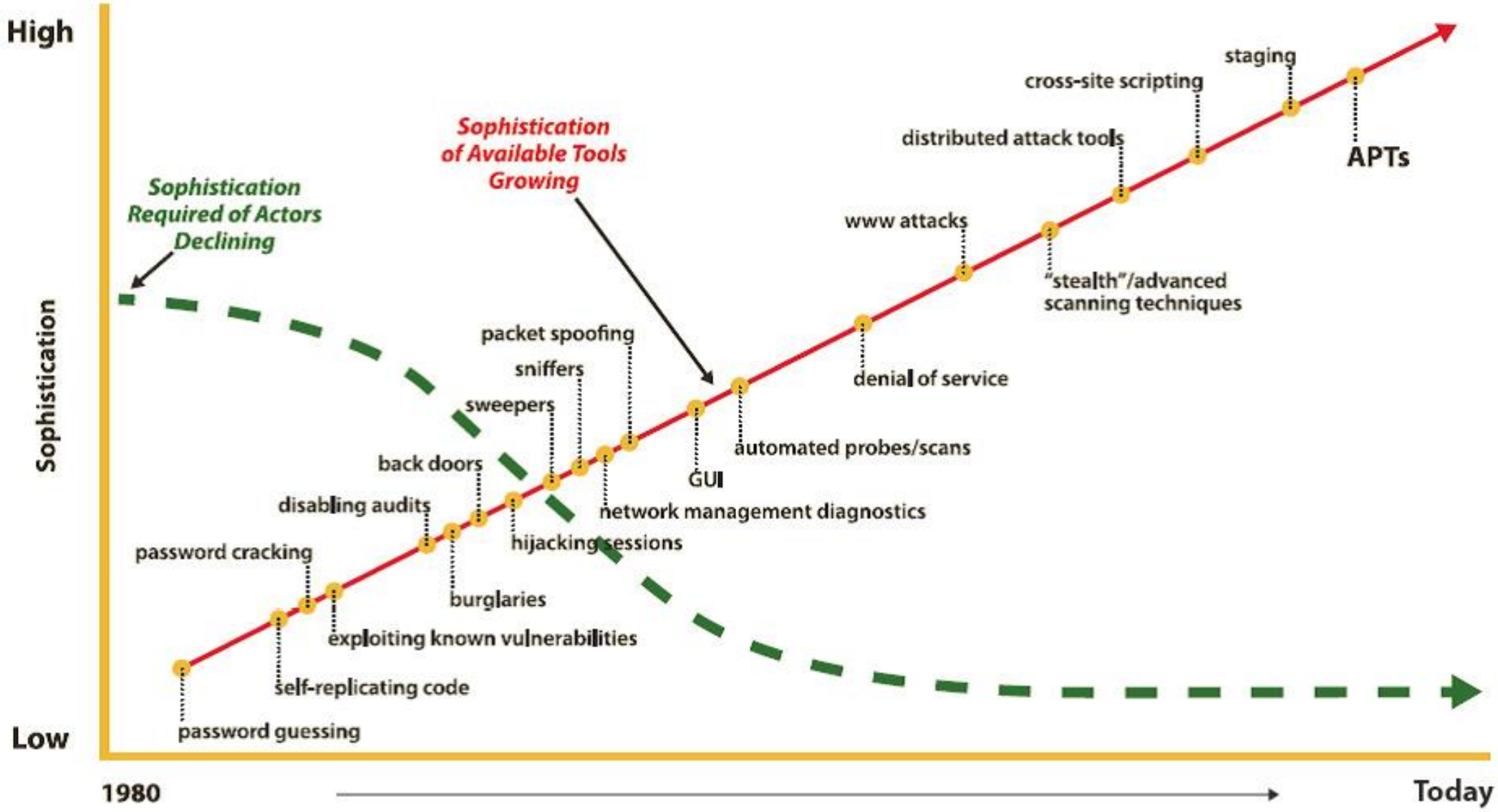


Image: https://newspaceeconomy.ca/

Adversaries & their Tools Security Evolution



source//www.csiac.org

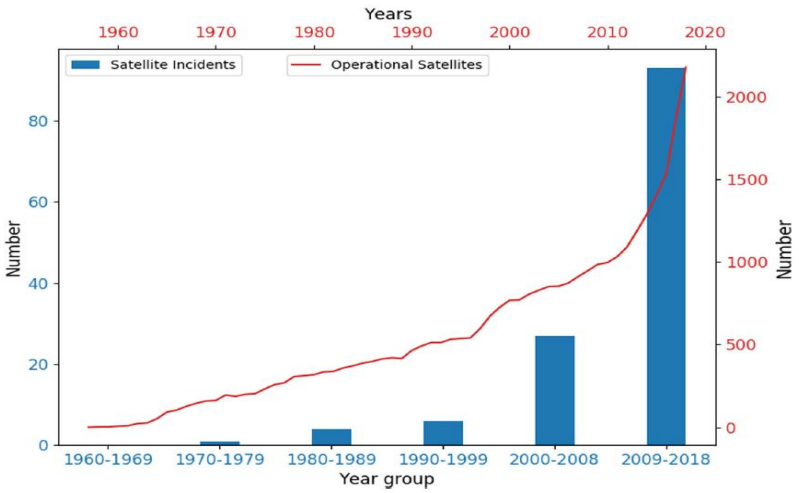
Space Security Context

Space systems are now more visible than ever

Experience the same issues as IT & OT

The domain related to space is evolving

Space systems have increasing risks



INTEREST, MOTIVATION & INCIDENTS ARE INCREASING

	Category	Frequency
Segment	Ground	83
	Space	8
	Data communications	38
	Unknown	2
Sector	Government	91
	Commercial	28
	Civilian	11
	Military	11
Incident type	Jamming	19
	Eavesdropping	3
	Spoofing	3
	Control	4
Target	CNE	30
	Hijacking	16
	Phishing	3
	Internet hijacking	1
	Denial of service	3
	Theft/loss	48
	ASAT incident	3

Space International Context

- In the last fifty years Satellites and Space system/service have acquired a much more important and global key role than what is *perceived* today
    - Space is a fundamental pillar of any State in the world in terms of Economy, Security, Sustainability, Energy, Civil Protection and in the daily life of citizens.
- Satellites and Space systems/services are a political driver
- Space is a critical global ecosystem;
    - Vulnerable, subject to be a target of an attack, to the detriment of critical services for a State and its citizens;
    - Powerful, to be used as an instrument to launch or facilitate an attack;

Space Domain needs to be Secure

Secure Environment – Secure Design and Development – Secure Operations

AGENDA

1.

2.

ESA Context

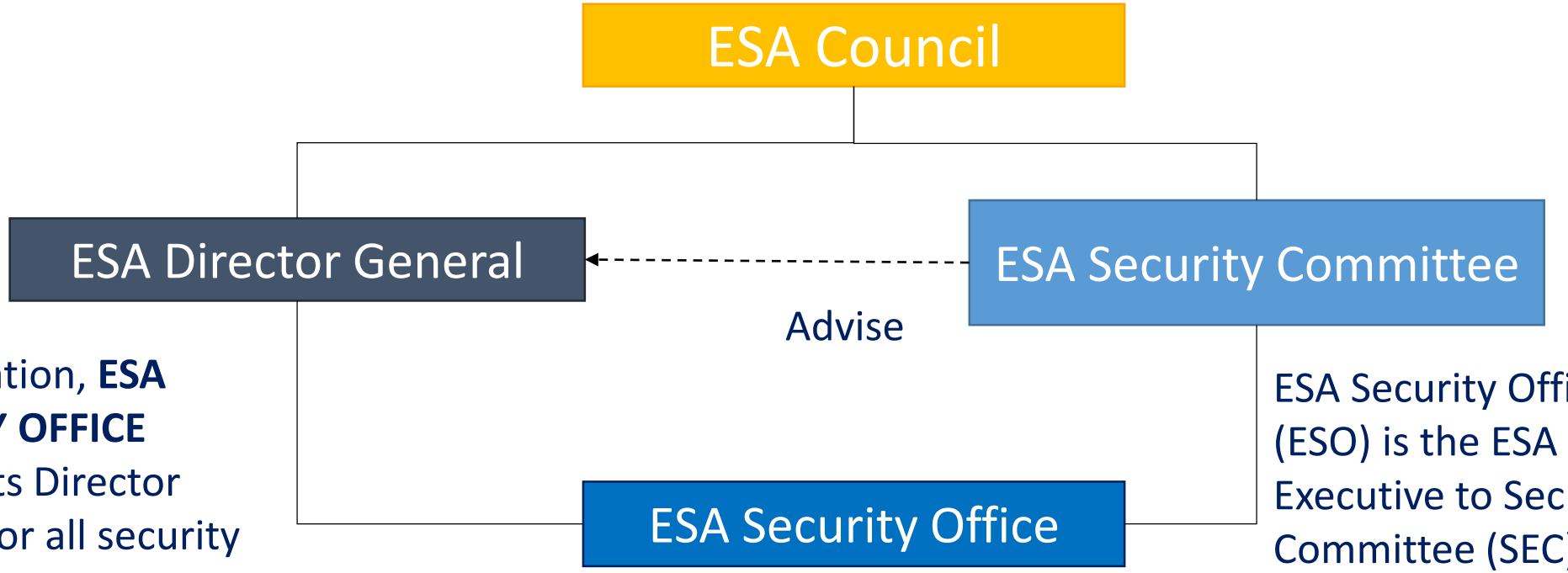
3.

4.

5.

Space Programme Security – Governance

- High Level view of the Security Governance in ESA



By delegation, **ESA SECURITY OFFICE** represents Director General for all security matters

ESA Security Office (ESO) is the ESA Executive to Security Committee (SEC)

ESO is the Security Authority *for ESA*

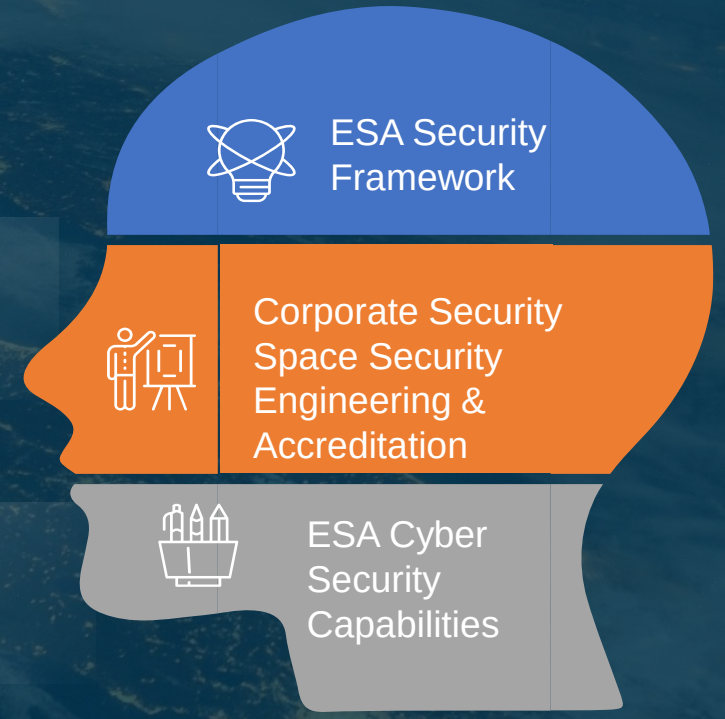
Security Objectives for ESA

- Security in ESA is conceived to give a high level of assurance to its Member States and International Stakeholders,

ESA Security Objectives:

1. Protect ESA Member States' investments in space

2. Protect ESA Image and Mission



Capability to provide secured space systems, designed, developed and accredited in a secured environment, through a holistic, coordinated approach

ESA Security Framework

1 Security Policy Regulations and Agreement

2 Space and Corporate Security Engineering

ESA Security Agreement

Agreement between the States Parties and the European Space Agency for the protection and exchange of classified information approved by ESA Council on 13 June 2002 and entered into force on 20 June 2003

ESA Security Regulations (2020)

Which identify the basic security principles and minimum standards to be applied by the European Space Agency.

ESA Security Directives (2020)

Directly derived from the ESA Security Regulations, they provide in a single source, the regulations and guidelines to assure the correct application of security and the safeguarding of information within the Agency.

3 Cyber Security Resilience and Technology

AGENDA

1.

2.

3. Cyber Activities

4.

5.

ESA Cyber Security Strategy

Based on an ESA Cyber Security Strategy

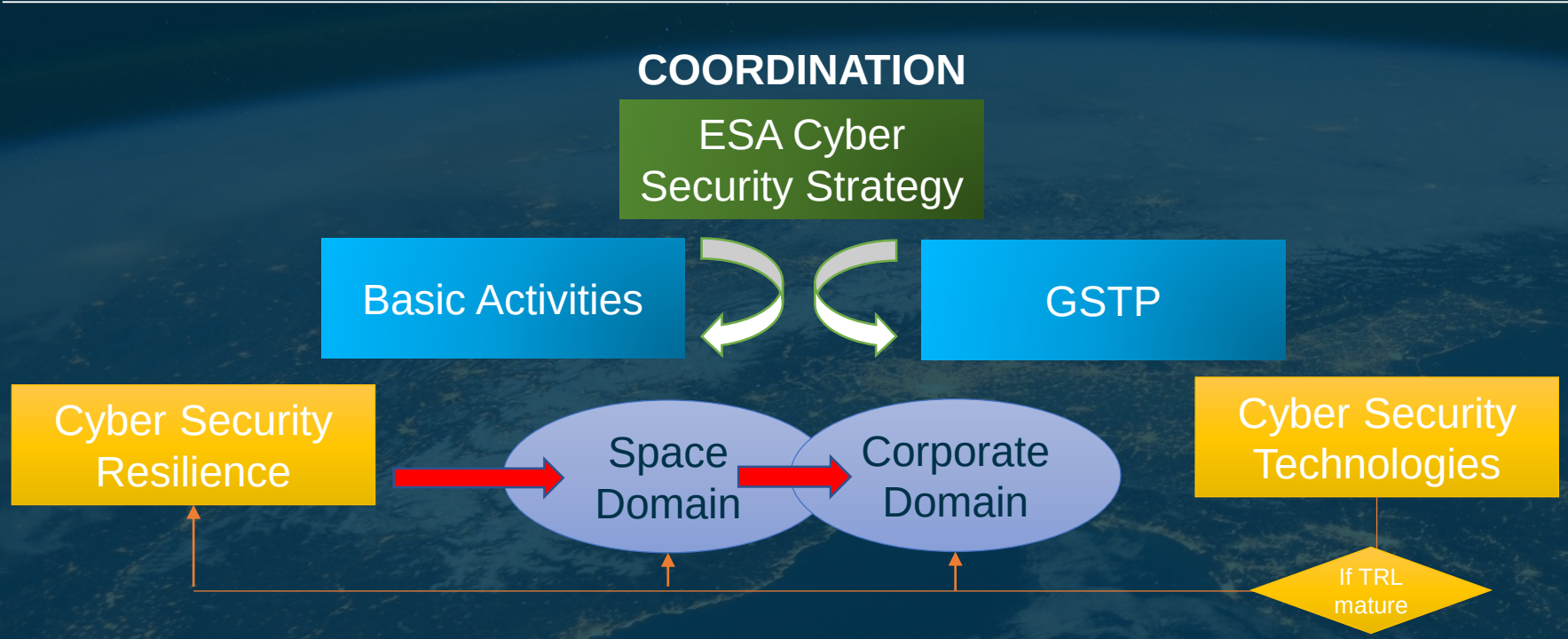
- Focused to mitigate the Security Risk of European Space Agency
- Short (2022-2023) medium (2023-2025) and long term (2023-2027) scope

CYBER SECURITY RESILIENCE

- ❑ **Cyber Security PREVENTIVE technologies** (how ESA can prevent or detect a potential Threat or Vulnerability affecting the ESA corporate and space mission assets) addressing the Cyber Security Operational Centre (C-SOC), the Security Cyber Centre of Excellence for Test, Validation and Qualification (SCCoE), and the Cyber Security Critical Assets as ESOC OPS NOC
- ❑ Cyber Security RESPONSIVE technologies (how ESA can respond or be protected from a potential Threat and its potential reaction) addressing the ESACERT capabilities

CYBER SECURITY RESEARCH AND DEVELOPMENT (R&D) New Technologies

ESA Cyber Security Strategy



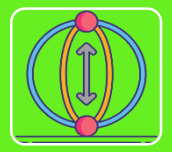
Cross-Directorate Agency Initiatives for Cyber

R&D Cyber Security Technology

Security Building Blocks for Satellites

- Integrity and authenticity module
- Reconfigurable, upgradable Crypto
- Security Avionics Bus
- Satellite Sandbox
- Endpoint Security Protection
- Reference Satellite Security Architecture
- Confidential Computing Assessment

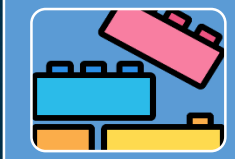
Post Quantum Cryptography



- Assessment, Adoption, Implementation & testing of PQ Cryptographic Algorithms and Solutions

Supply Chain

CCSDS Building Blocks



- SDLS, SDLS EP building blocks – second gen
- CCSDS DTN BSP Building Block
- IP-over-CCSDS with IPSec profile building block

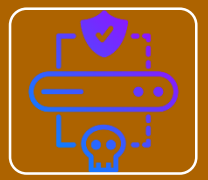
RF Firewalls for Satellite

- RF Firewall for Onboard GNSS Receiver
- RF Firewall & Threat Locator

Software Interface Simulation Module

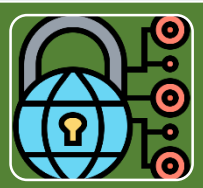
- Simulation Extension SW block for Mission Operations

Zero Trust for Mission Ground Segments



Federated Operations Security Arch

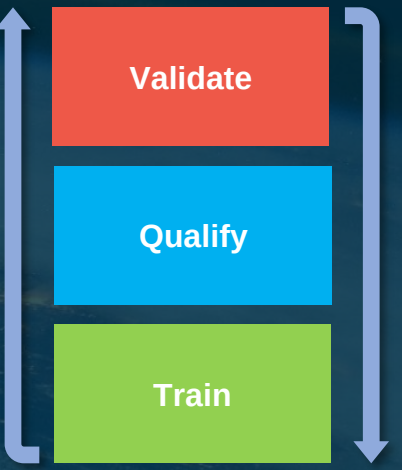
Secure Systems Engineering Framework



- Secure System Engineering Toolset for Mission Operations

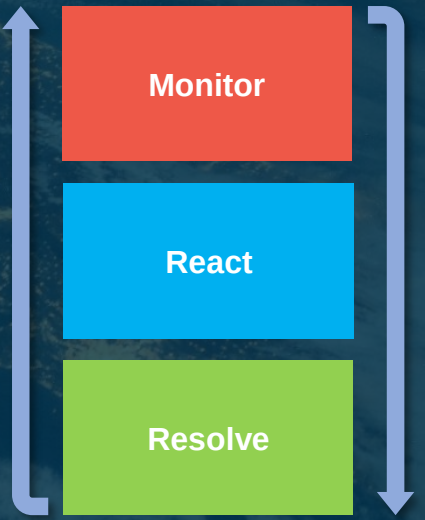
Cyber Security Ongoing Developments in ESA Security Office

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. It will also represent the focal point for a Security expertise and sharing, training as well as support to developers assessing security risk;



Cyber Security Operations Centre (CSOC), complementing the state-of-the-art Computer and Communications Emergency Response Team (CERT), the Cyber Security Operations Centre (CSOC) will provide an ESA-wide cyber monitoring and management capability. CSOC will monitor and track relevant information and events with the objective of maintaining the overall Agency security posture. The CSOC will detect security incidents and support the readiness of the organisation's defensive capabilities and support cyber intelligence sharing.

The CSOC 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.



Security Operations Centre (SOC) Context

End User / Tenant Monitored Systems

End User / Tenant C-SOC Customer Interface

C-SOC Core System

IT

CSOC Peripheral Element (PE)

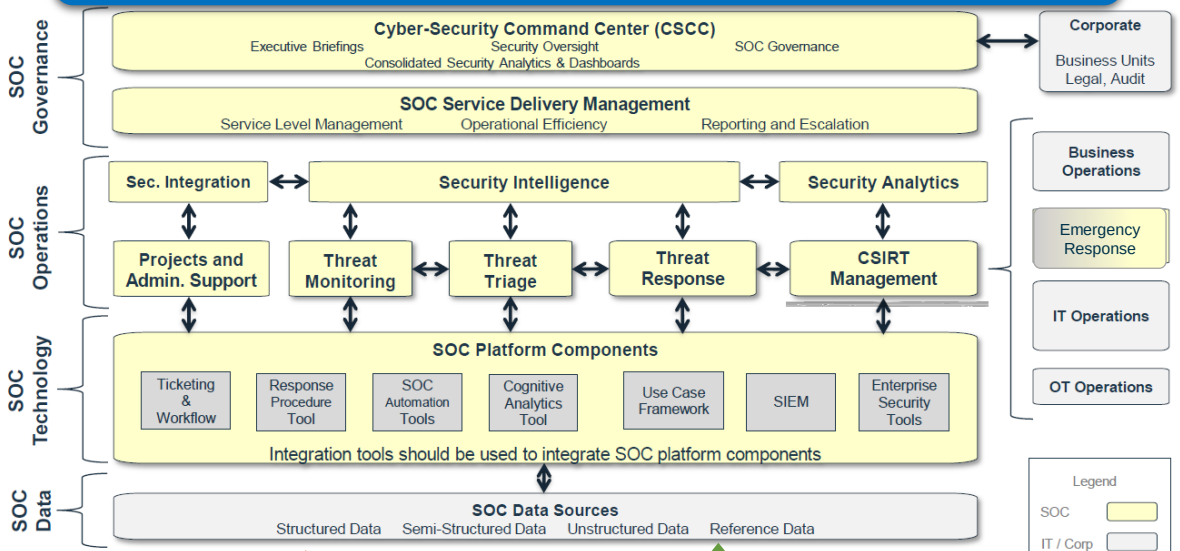
C-SOC Cyber – Portable Operations Platform (C-POP)

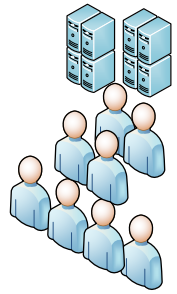
Incident Prevention, Detection, Response, Recovery

Tickets, Requests, CTI, Assets, Incidents

Incident Tracking, Reporting, Dashboards, CSOC Service access

Events, Alarms, Data, Requests, Status, Audit Information





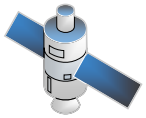
Threat Intelligence

Trusted Partners

SPACE Related Cyber Threat Intelligence Sharing

SPACE THREAT PARTICIPANTS


Launch


Space


Communications


Engineering

Supply Chain


IT

OT

Threats

Incidents

Vulnerabilities

Reports

Papers

Standards

Training

Space Cyber Threat Hub

esa

Alerts
Standards
Knowledge

POSSIBLE PARTNER INSTITUTIONS

esa

EUROPEAN DEFENCE AGENCY

enisa European Network and Information Security Agency

CSIRTs NETWORK

Bundesamt für Sicherheit in der Informationstechnik

SGDSN SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

cnes

ESO

LSN LUXEMBOURG SPACE AGENCY

Netherlands Space Office

PORTUGAL SPACE

ASI Agenzia Spaziale Italiana

Norsk Romsenter Norwegian Space Agency

NSERC CRSNG

Rymdstyrelsen Swedish National Space Board

SPACE ISAC

rosa

cnes CENTRE NATIONAL D'ETUDES SPATIALES

RYMDSTYRELSEN Swedish National Space Board

Norsk Romsenter NORWEGIAN SPACE CENTRE

agenzia spaziale italiana

CBK

INTA

FFG

DTU

FCT

ENTERPRISE IRELAND

Magyar Űrkutatási Iroda

LUXINNOVATION

Tekes

belspo

IAAΔET

DLR

Ministry of Economic Affairs and Employment of Finland

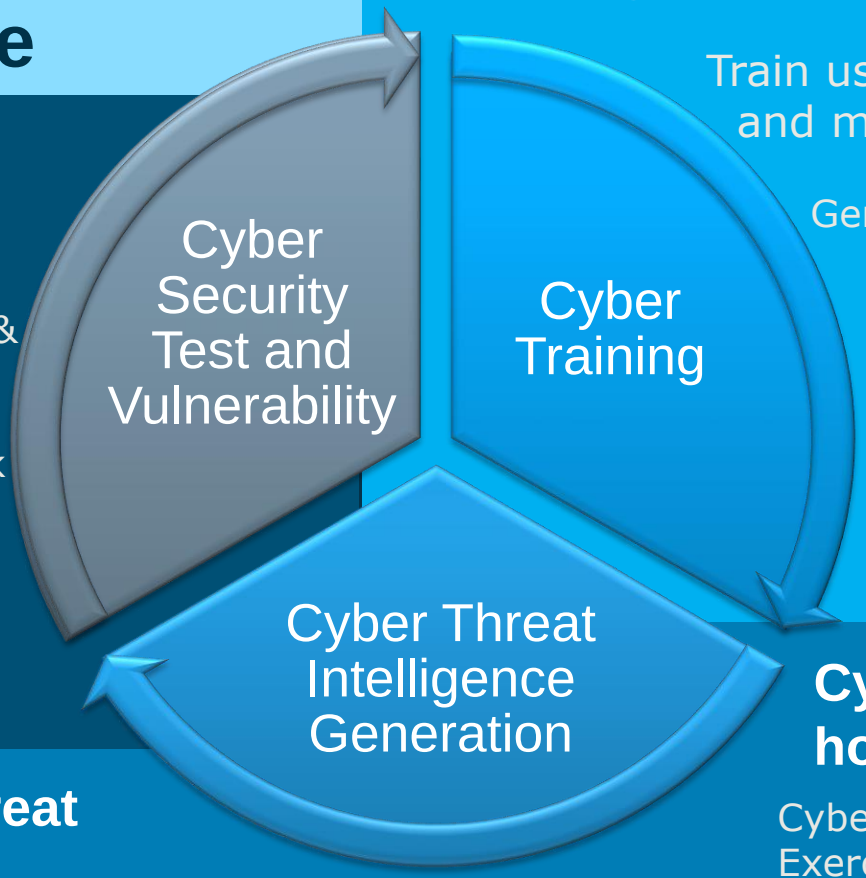
+ many others

ESA Space Security Cyber Centre of Excellence

ESA Space Security Cyber Centre of Excellence

Cyber security test and vulnerability assessment

Independent security testing of space systems & products
Vulnerability analysis, penetration testing
Tools to assist system security qualification, risk & validation
Operations security procedure development validation and experimentation
Certification & Accreditation support



Cyber awareness & training

Train users, operators, engineers and managers on IT & Space Security

General awareness training
Expert (e.g. ISO, SRMP) training
Advanced security education
Security-by-design principles
Secure network implementation & configuration
Security incident management
Security forensics

Cyber security exercise hosting & participation

Cyber-Sim exercise hosting
Exercise planning and coordination

Cyber security research, threat intelligence generation

Collaboration tools for ESA & partners for Threat Intelligence analysis and generation

Secure solution research and experimentation
Vulnerability and malware research
New product experimentation, testing

ESA Cyber Security Resilience Implementation

ESEC-ESOC
CSOC MASTER & BACKUP

ESEC

ESA
EXTERNAL
STAKEHOLDER

Threat & Security Analysis

Cyber System Monitoring

Cyber Training, Test and Validation

Specific Cyber Engineering R&D

Cyber Emulated Environment

Security Policy development

ESA
INTERNAL
STAKEHOLDER

ESEC-ESRIN
ESACERT MASTER & BACKUP

ESRIN

US DEFCON & ESA HACK-A-SAT

- Hack-a-sat (USAF Research Laboratory & Space Systems Command Challenge since 2020)
- Results published at DEFCON

https://hack.cysat.eu/

https://www.afrl.af.mil/News/Article-Display/Article/3002762/space-security-challenge-2022-hack-a-sat-3-registration-opens/
https://hackasat.com/

- ESA OPS ran a small event in 2022 and a live ethical hack in 2023!
- See google ☺

AGENDA

1.

2.

3.

4. Security Standards

5.

Security Frameworks

Most Security Frameworks are non-prescriptive

- **ISO 27000** gives overall guidance
- CCSDS provides examples, even Blue Book standards often provide recommendations rather than instruction
  - **CCSDS Security for Mission Planners (350.7)**

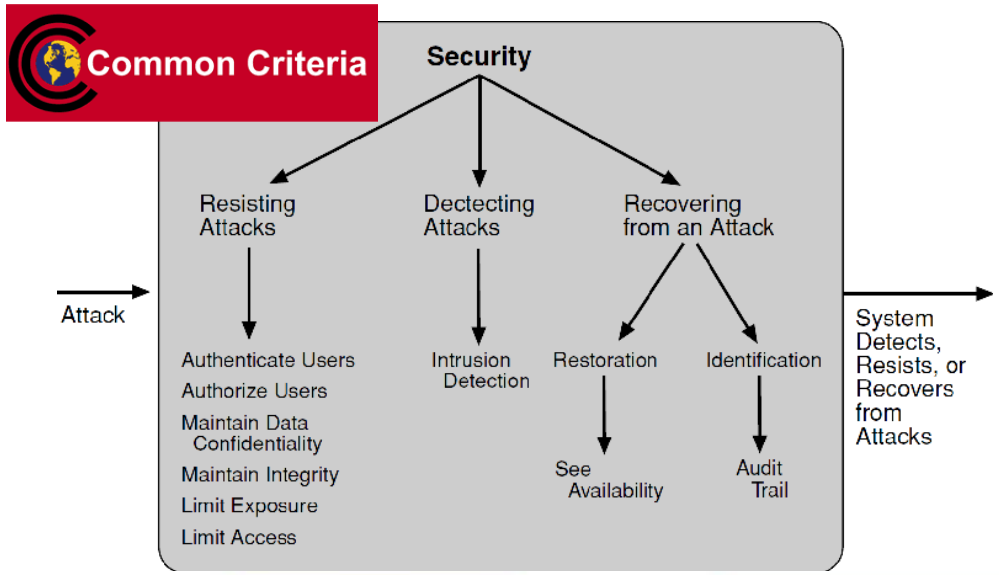
- **NIST Cyber Security Framework** (CSF) also a framework
  - Maps onto common supporting standards such as NIST 800-53b.

- **NIST 800-53b** is more prescriptive control catalogue
  - has additional guidance for implementation (e.g. patch mgmt., TLS, PKI ..) and needs tailoring
  - Mandated for federal projects
  - CNSS provides some space overlays

- **FEDRAMP +** is for Cloud, based on NIST 800-53 augmented with specific controls for providers of cloud services.

Other Sources of Cyber-Security Controls

- Preschern, Christopher. "Catalog of security tactics linked to common criteria requirements." (2012).

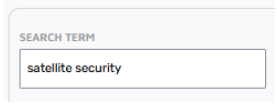


Common Criteria SFR Classes \ Security Tactics	Authenticate Users	Authorize Users	Maintain Data Confidentiality	Maintain Integrity	Limit Exposure	Limit Access	Intrusion Detection	Restoration Availability	Identification Audit Trail
FAU (Security Audit)							X		X
FCO (Communication)									X
FCS (Cryptographic Support)	X								
FDP (User Data Protection)	X	X	X	X				X	X
FIA (Identification&Authentication)	X	X							
FMT (Security Management)	X	X		X					
FPR (Privacy)									
FPT (Protection of the TSF)			X	X			X	X	
FRU (Resource Utilisation)				X		X			
FTA (TOE Access)	X								
FTP (Trusted Path/Channels)	X		X	X					

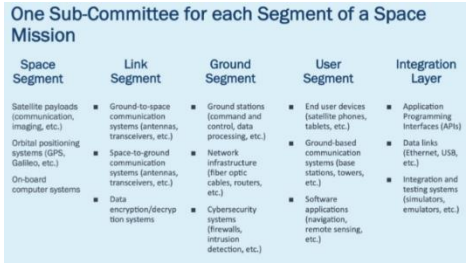
Table I: Mapping of the Common Criteria SFR classes to security tactics

https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf

Other Sources of (Space) Cyber-Security Controls (ii)

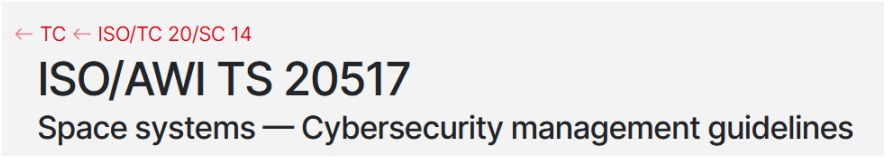


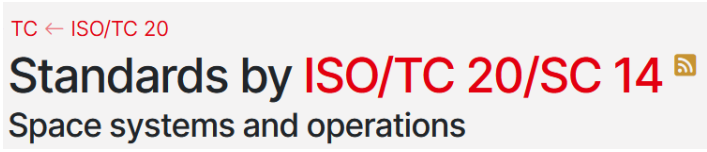
https://www.etsi.org/



INTERNATIONAL TECHNICAL STANDARD FOR SPACE SYSTEM CYBERSECURITY - IEEE P3349 WORKING GROUP (WG)

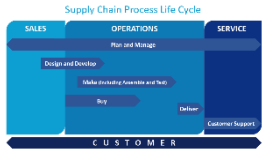
https://sagroups.ieee.org/3349/





https://www.iso.org/committee/46614/x/catalogue/

https://www.ietf.org/



https://scmh.iaqg.org/

NIST Space Related Guidance

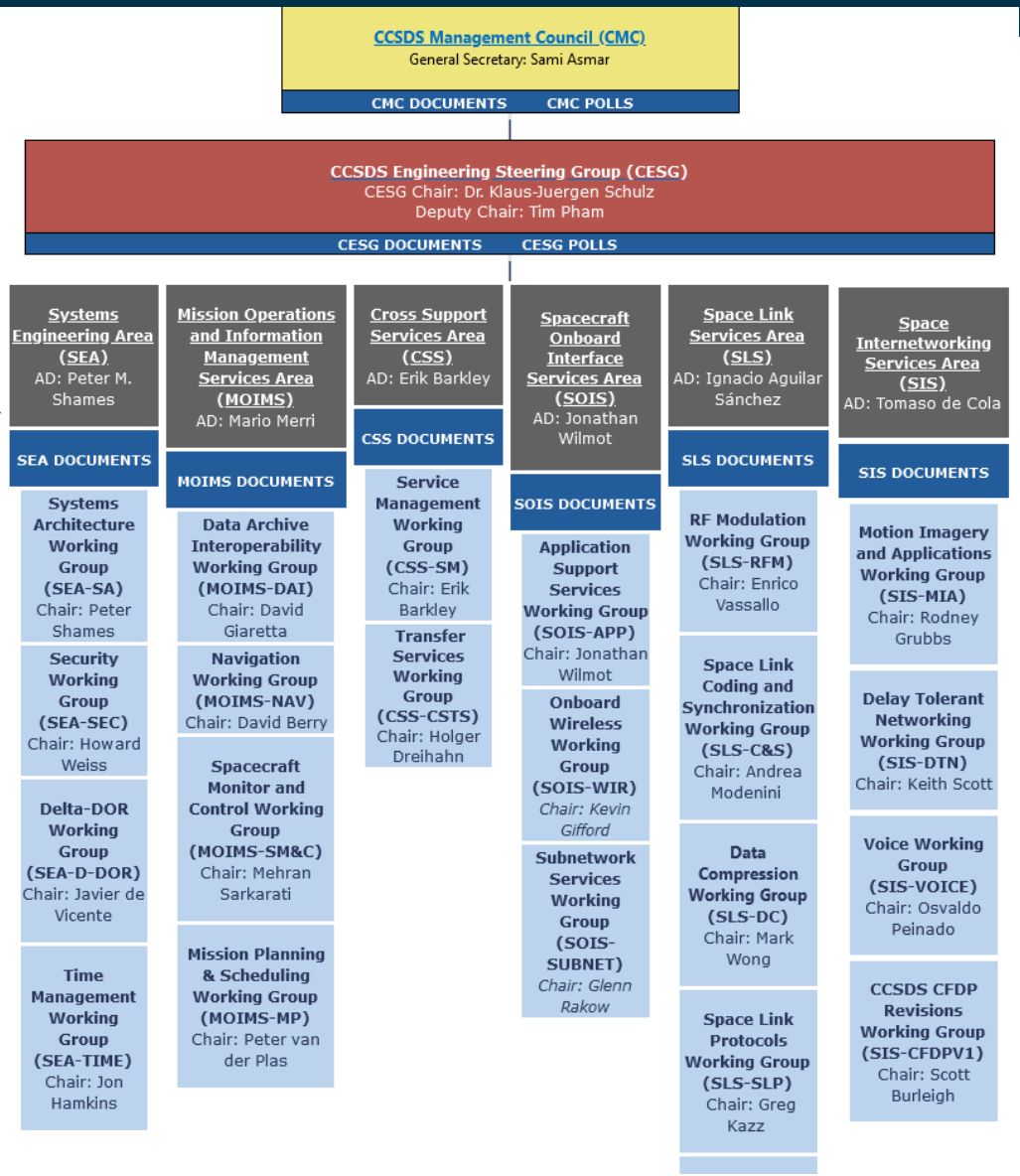
- *(NIST IR 8270) Introduction to Cybersecurity for Commercial Satellite Operations.*
- *(NIST IR 8323)* - Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services.
- *(NIST 8401) Satellite Ground Segment: Applying the Cybersecurity Framework (CSF) to Assure Satellite Command and Control*
- **Hybrid Satellite Networks: Cybersecurity Draft Annotated Outline**

Security Space Standards CCSDS

- Consultative Committee for Space Data Systems (CCSDS)
- The CCSDS **Security Working Group is within the System Engineering** Area

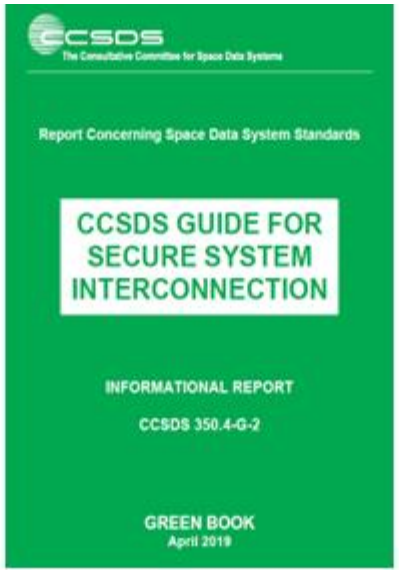
System Engineering Area

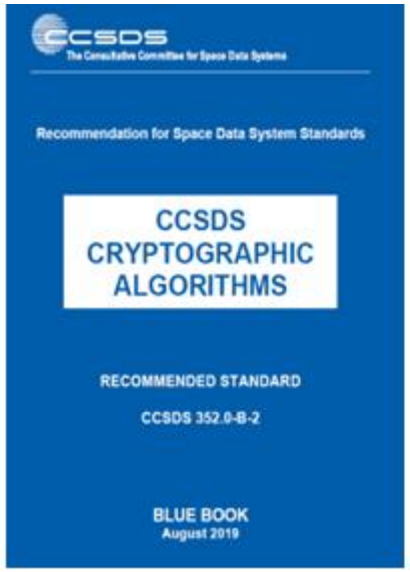
Security Working Group



Security in Engineering Space lifecycle – CCSDS (ii)

CCSDS Top 6 for security

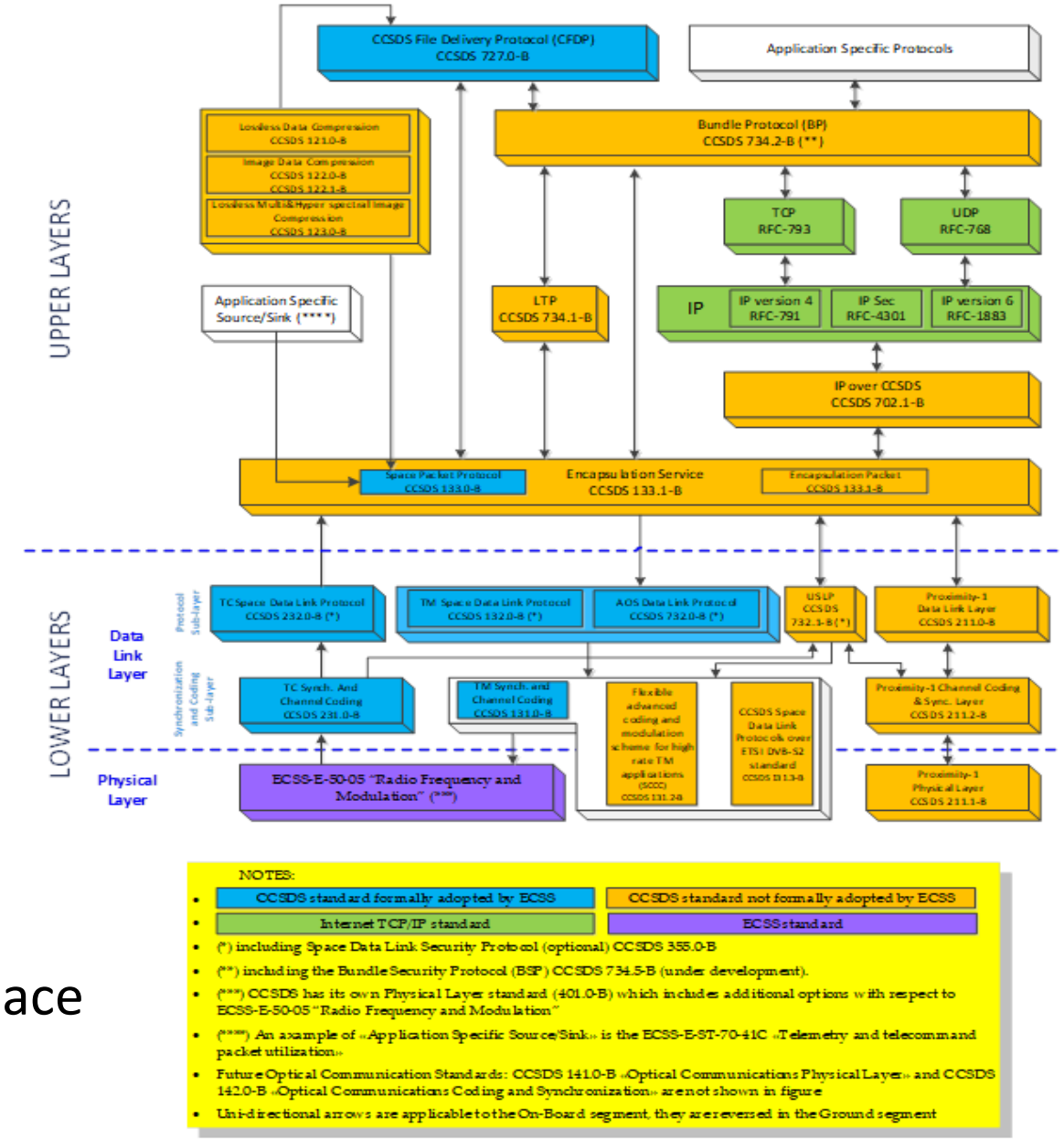




CCSDS 35x are dedicated security focused guides & recommendations

Security in CCSDS toplogy

- CCSDS includes Link security but as an *optional* component
- CCSDS 131.0-B-3 discusses security issues with TM Synchronization and Channel coding CCSDS blue books CCSDS 355, 734.5
- TC, TM and AOS Space Data Link Protocols (CCSDS 232.0, 132 and 732)
- Bundled Protocol has the related Bundled Security Protocol (BSP) 734.5 under finalisation



ECSS/CCSDS Telecomms Protocols Space

https://ecss.nl/standard/ecss-e-st-50c-rev-1-communications-1-march-2021/

CCSDS Cryptographic Recommendations are quite open

Protection Type	Algorithm/Mode	Key Size and notes
Encryption	AES-CTR	Key size of 256-bits for future implementations, 128-bits for current ones
Authenticated Encryption	AES-GCM	Key size of 256-bits for future implementations MAC size of 128-bits
Authentication	Any hash, cipher or digital signature.	Left open with some recommendations below
	SHA-256	Normal
	SHA-224, SHA-384, SHA-512, RIPMD-160 …	alternative by communicating parties
Cipher based Authentication	AES-CMAC	with 256-bit key (existing may use 128, 192 or 256-bit keys)
	AES-GMAC	when only authentication required.
Digital Signature	DSS	(includes DSA, RSA & ECDSA)
	RSA	at least 4096-bit keys for future implementations, possible to have 2048-bit keys for current implementations
	DSA or ECDSA	may be used

Irving Interpretation of CCSDS 352-0-B-2 Recommendations

ECSS – European Cooperation for Space Standardization

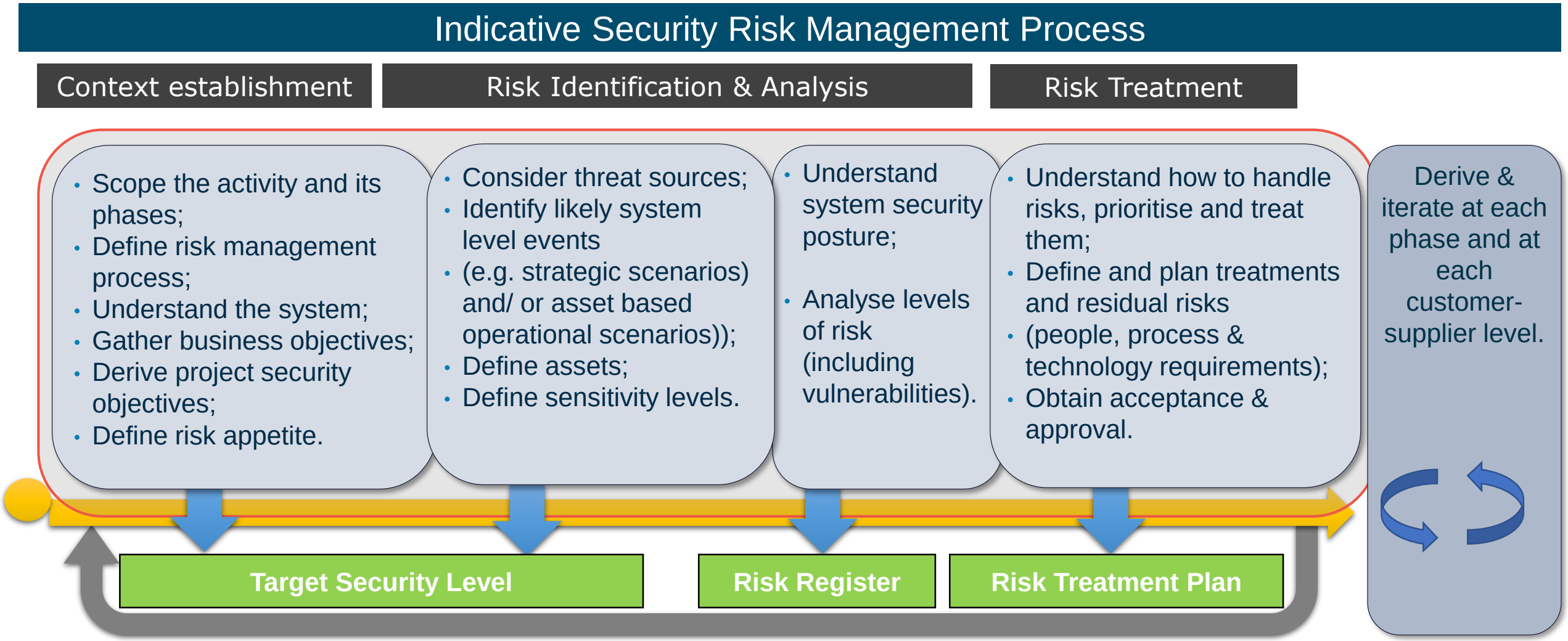
- Collaboration from ESA, European space industry and several space agencies.
- ESA is major contributor to this endeavour.

- Security is quite new.
- ECSS-M-80 on Risk Management – mentions security, but method is aligned well with ISO27000
- ECSS-E-40 for software engineering – last update (end 2022) under public review adds security
- ECSS-Q-80 for PA for software – under internal review to add security

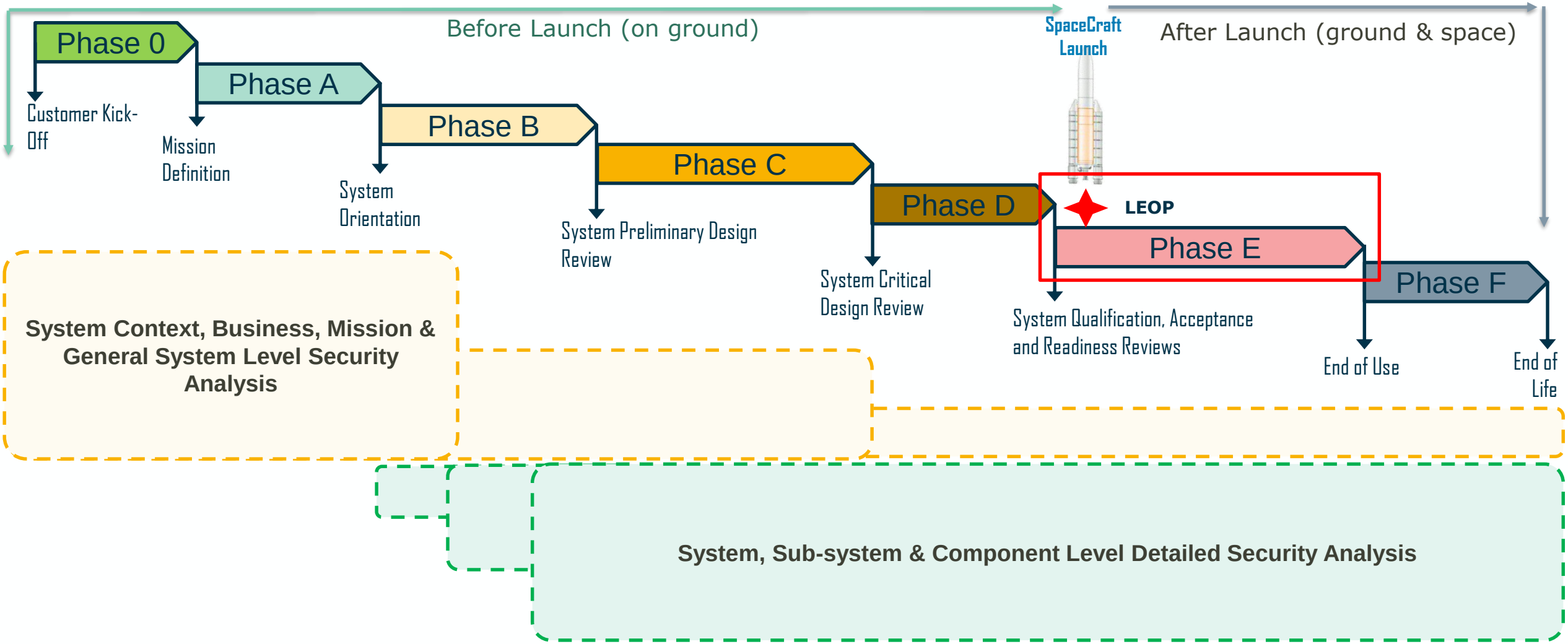
- **NEW STANDARD – System Security Engineering**
- First Draft from dedicated working group from ESA, European Institutions & European Industry is ready
- - Under review by Secretariat
- - Now under public review on 21 June, comments before 8 Sept 2023.

Risk Assessment example process (from ECSS draft)

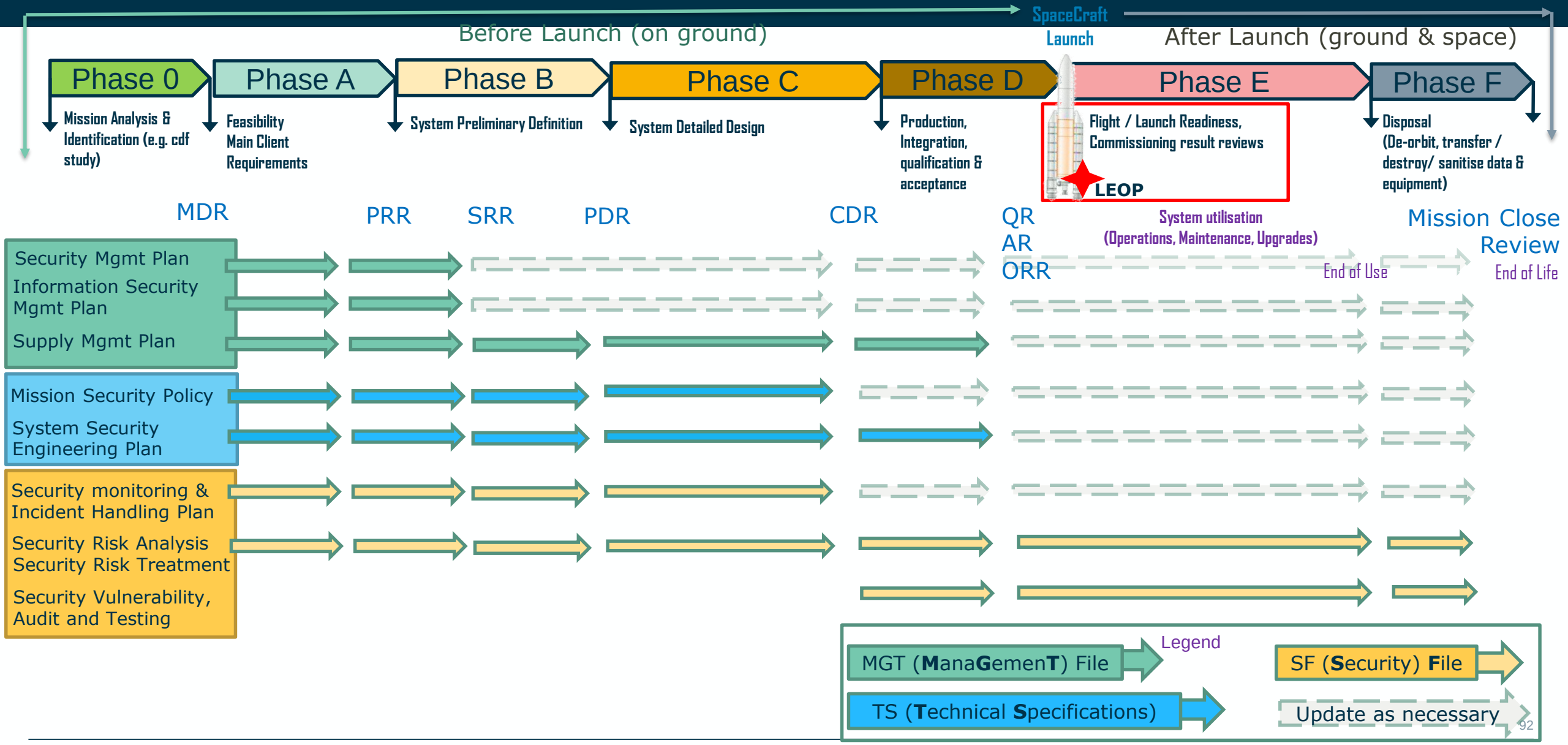
Indicative Security Risk Management Process



Level of Detail and Refinement by Phase (from ECSS dr)



Level of Detail and Refinement by Phase & doc (ECSS dr)



Security Related Document and Phase (ECSS draft)

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	KOM	SRR	PDR	CDR	QR	AR	ORR
MGT	Information Security Management Plan	✓	✓					
	Security Management Plan	✓	✓					
	Supply Management Plan	✓	✓	✓	✓	✓	✓	
TS	Mission Security Policy	✓	✓	✓	✓			
	System Security Engineering Plan		✓	✓	✓	✓		
SF	Security Risk Analysis		✓	✓	✓	✓	✓	✓
	Security Audits					✓	✓	✓
	Security Vulnerability Analysis and Testing Report					✓	✓	
	Vulnerability Assessment Reports					✓	✓	✓
	Penetration Testing Reports					✓	✓	✓
	Security Risk Treatment Plan		✓	✓	✓	✓	✓	✓
	Security Monitoring and Incident Handling Management Plan	✓	✓	✓	✓			

Debris Mitigation Guidelines

- https://www.esa.int/Space_Safety/Space_Debris/Mitigating_space_debris_generation

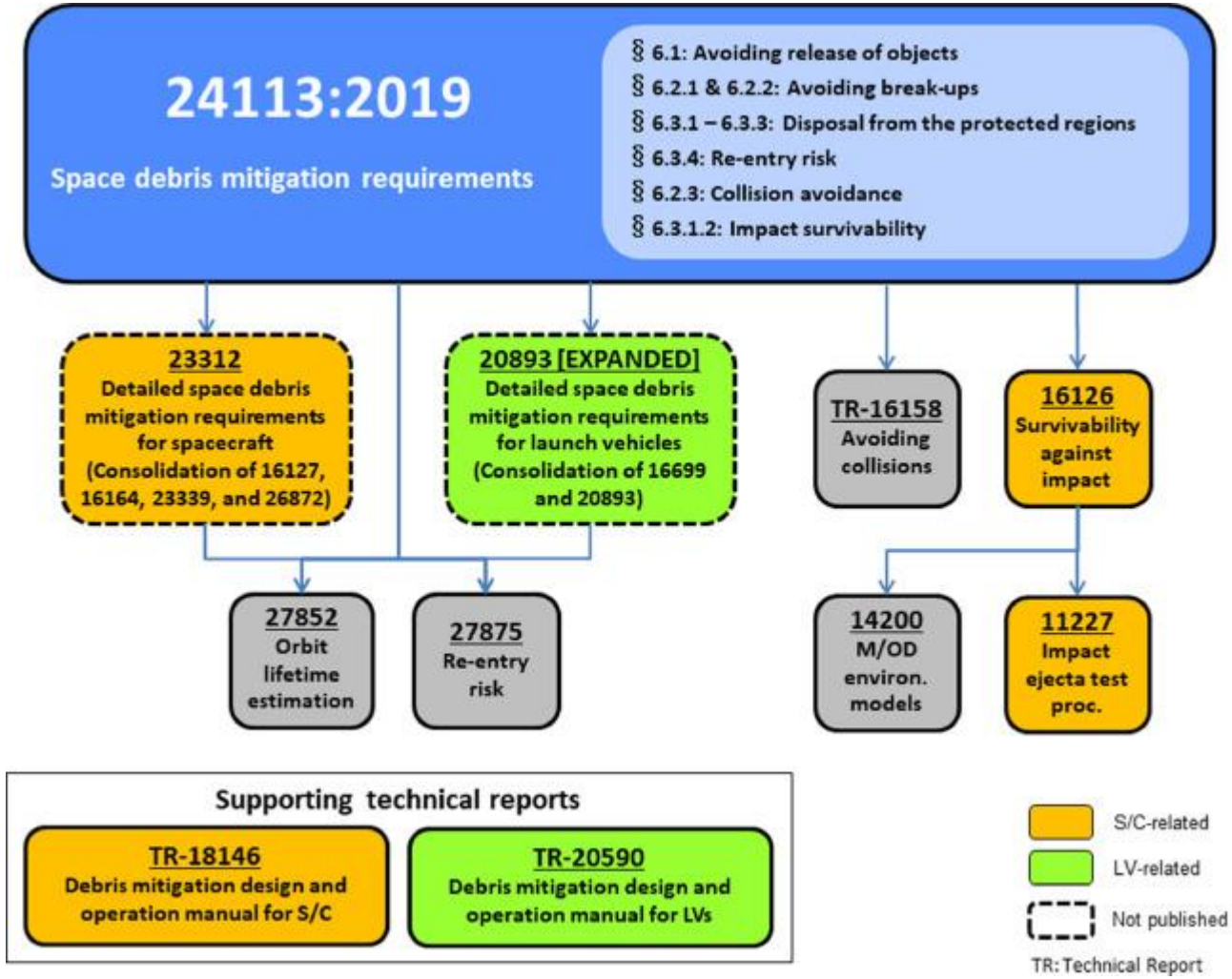
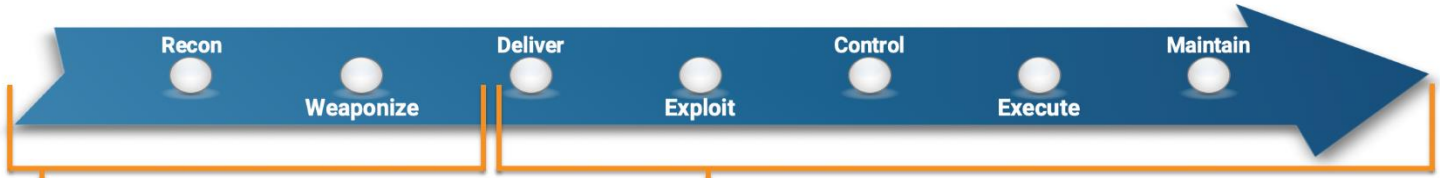


Image: Stokes et al 2020 "Evolution of ISO's space mitigation standards

Cyber Kill Chain, MITRE ATT&CK Framework

- **Useful to help with threat modelling** an complex playbooks to help
- **understand behaviours of attack**
- **track who is doing what & where**
- **assist in threat intelligence**
- **assist in identifying countermeasures and controls**



PRE-ATT&CK

- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organizational
- Weakness Identification
  - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

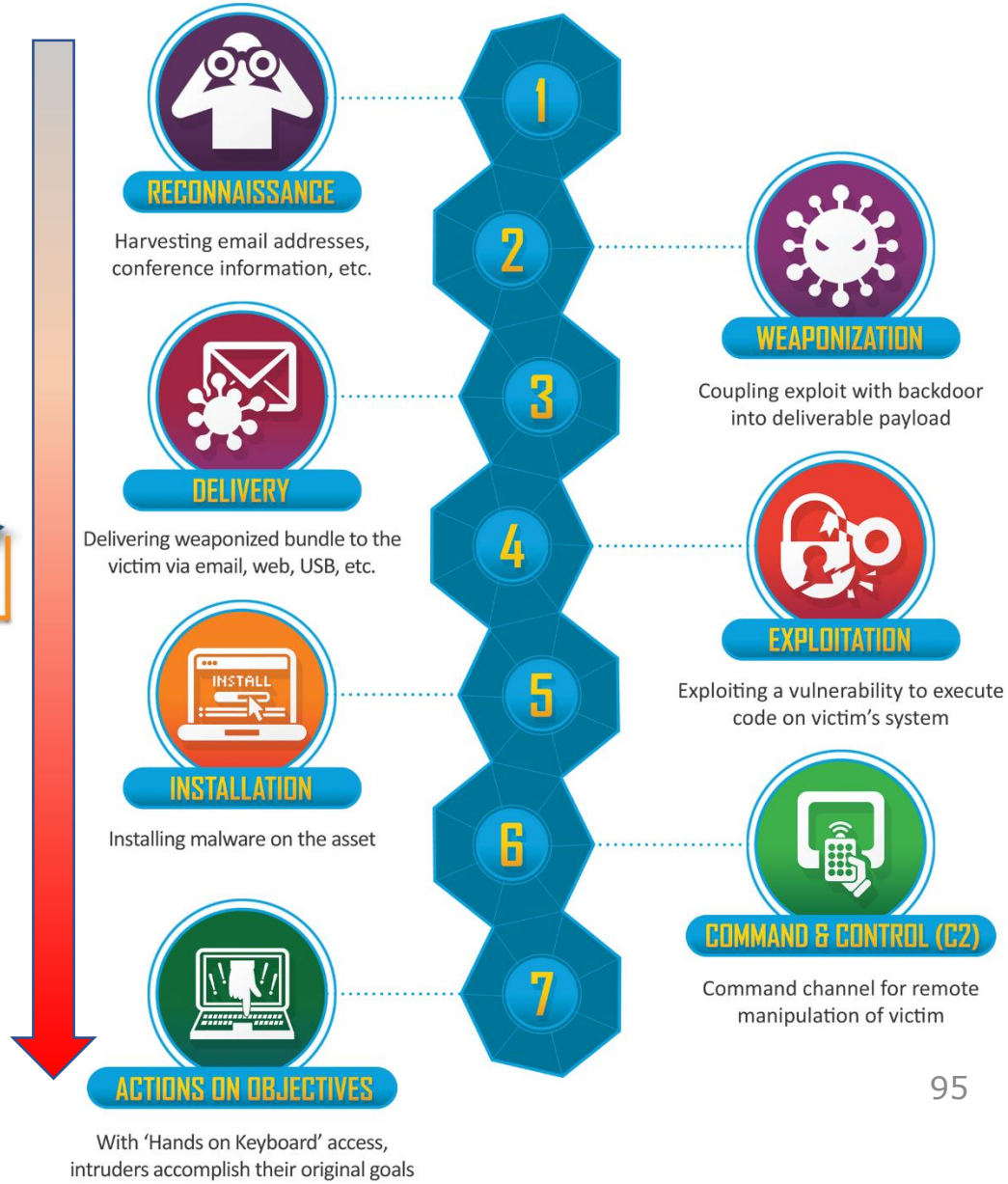


Image: lockheedmartin.com

MITRE ATT&CK Framework

- MITRE uses 3 tiers, to allow explanation of the activity based on the objective (or tactic)

Tactic {

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Distributed Component	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Byp... Acc...					Data Transfer Size Limits	Custom Comm... Co...
									Exfil...	

Technique

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.[1]

Drive-by Compromise
Technique

ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Procedure

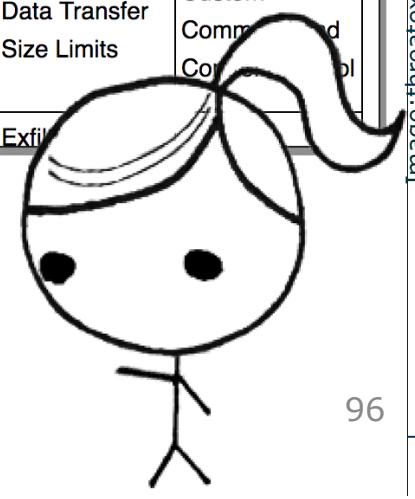


Image: threatexpress.com

MITRE ATT&CK Framework – example

- MITRE Tactics and techniques used by [APT Chimera during Operation Skeleton Key](), synthesis of hacker tools from a single group. Skeleton key malware is a

VPN using compromised password

Wmi to remotely execute commands
Powershell compromises for migrate & analysis
Schedule task to launch malware
Inject false credentials

Cobalt Strike malware

Net user commands

rdp valid account
Admin shares

Google appspot to host C2 server

Encrypt & compress data to send via C2

SPARTA TTP Framework (©Aerospace Corporation)

https://sparta.aerospace.org

Released Oct 2022, v1.3.1 in May 2023.

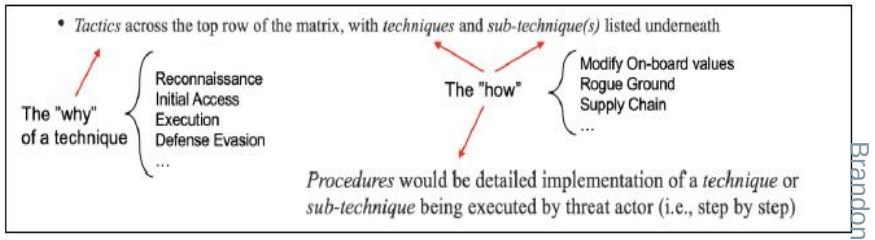
In collaboration with CCSDS and exchanges with ESA

Use Cases:
- Development
- Threat Intelligence
- Threat Modelling
- Education/Training

Now includes possible countermeasures

Space Attack Research & Tactic Analysis (SPARTA)

- Cybersecurity matrices are industry-standard tools and approaches for commercial and government users to navigate rapidly evolving cyber threats and vulnerabilities and outpace cyber threats
  - *They provide a critical knowledge base of adversary behaviors*
  - *Framework for adversarial actions across the attack lifecycle with applicable countermeasures*



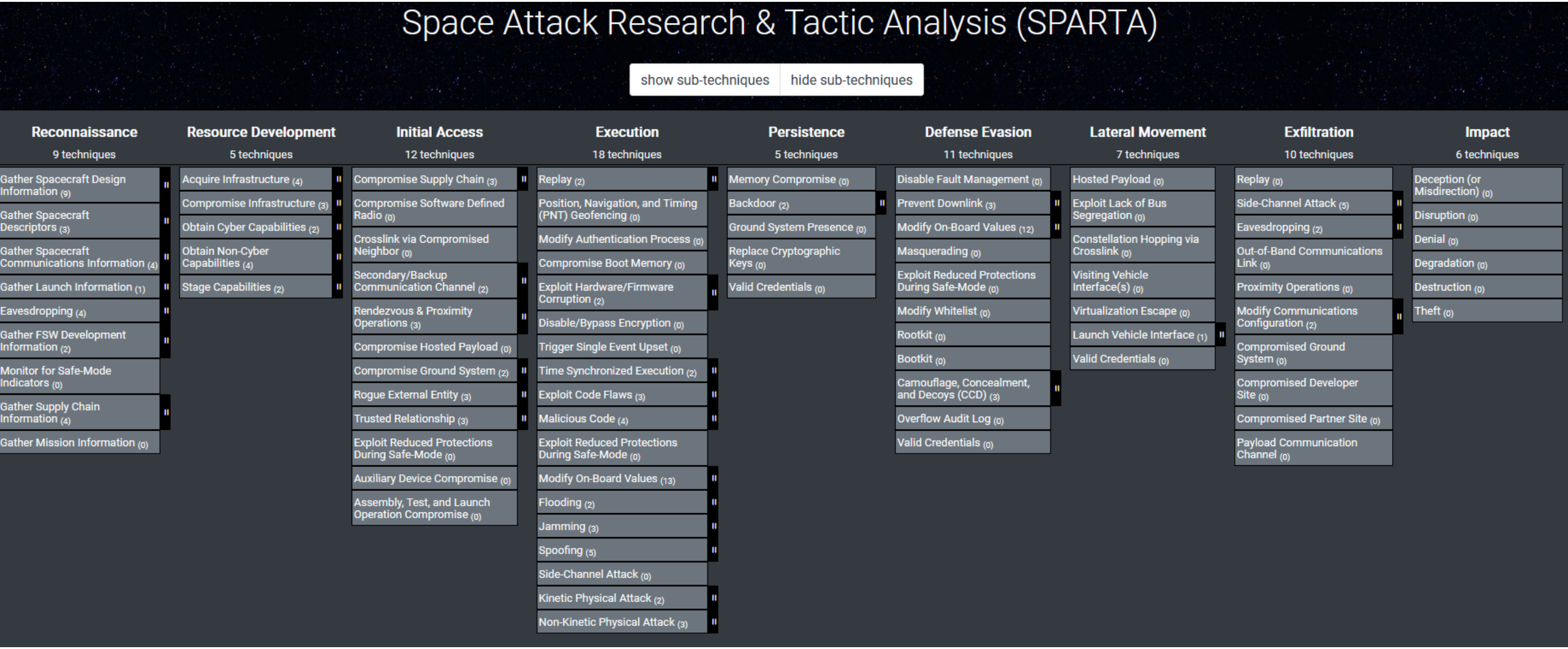
- Aerospace's SPARTA matrix is the first-of-its-kind body of knowledge on cybersecurity protections for spacecraft and space systems, filling a critical vulnerability gap for the U.S. space enterprise

SPARTA provides unclassified information to space professionals about how spacecraft may be compromised

"SPARTA - Space Attack Research and Tactics Analysis" Brandon Bailey, Brad Roeher, Randi Tinney - CyberSatGov2022, The AeroSpace Corporation, USA – www.aerospace.org

Attack for Space (Aerospace.org)

- https://sparta.aerospace.org/



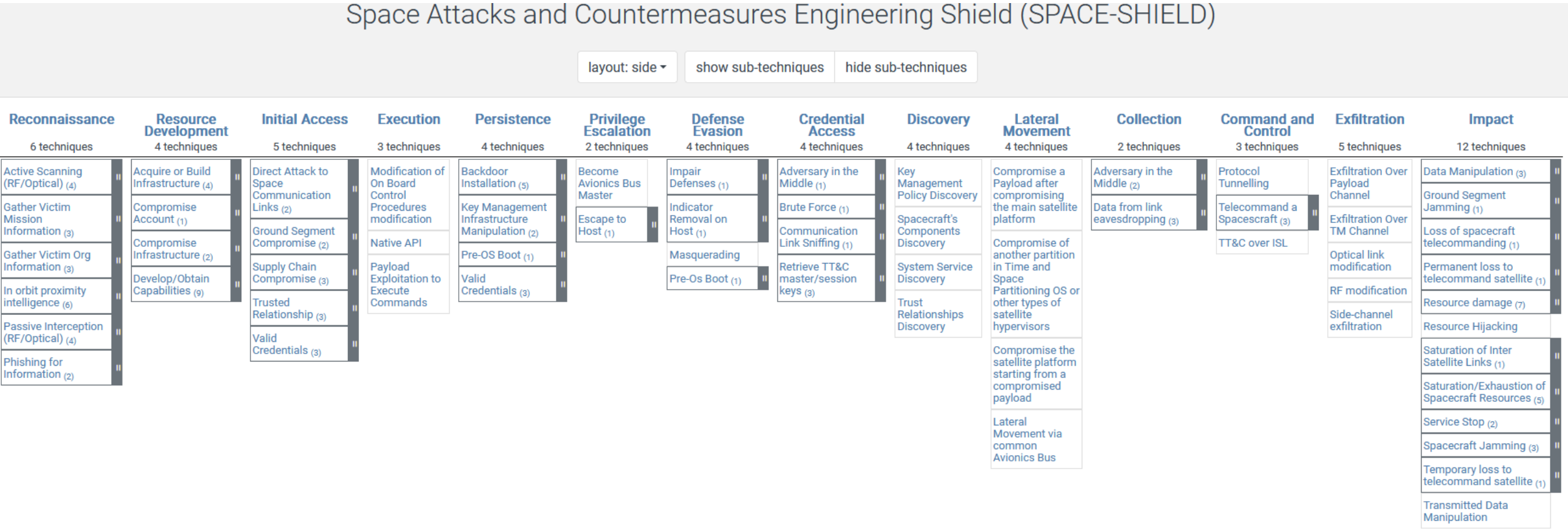
ESA SPACE-SHIELD

- Space Attacks and Countermeasures Engineering Shield

- A one-stop place aggregating potential attacking tactics, techniques, and sub-techniques for space systems:
    - To model (future) Space Threat Intelligence (STI) information
    - To identify needed defensive techniques and mitigations.
    - To develop new security technologies for space.
    - To identify security monitoring and logging needs
    - To assist system risk analysis.
- Aligned with SPARTA and CCSDS
- On-going work in collaboration with CCSDS

ESA Spaceshield

https://spaceshield.esa.int

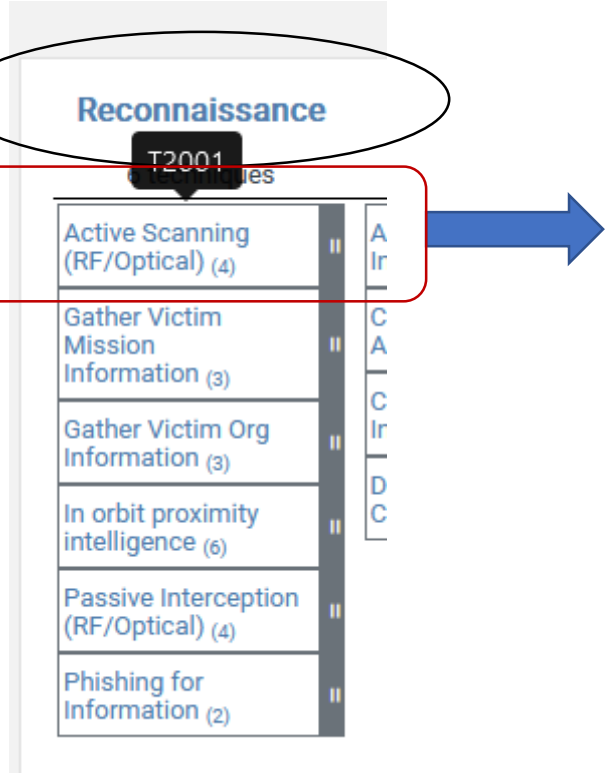


ESA Spaceshield - example

https://spaceshield.esa.int

Tactic

Technique



Procedure

Active Scanning (RF/Optical)

Sub-techniques (4)

The technique is the same of the Passive Interception, the difference is that the attacker initiates interaction with the space target trying to trigger potential responses (even error messages) by actively sending signals/packets. The scan can be similar to a "brute force" attack, in the sense that the objective is 'guess' the used frequencies and protocols to obtain a reply. This is why authentication is also included here as a mitigation measure (provided that it does not solicit any response to not authenticated signals). On the other hand, since sending telemetry data won't trigger any response due to their nature (even if they are fully compliant with the expected format), are not included here as a subtechniques.

Standard/references: [1] [2] [3] [4][5]

ID: T2001

Sub-techniques: T2001.001, T2001.002, T2001.003, T2001.004

Tactic: Reconnaissance

Platforms: Ground Segment, Space Segment, Space-link communication

Version: 2.0

Created: 25 August 2022

Last Modified: 21 April 2023

Mitigations

ID	Mitigation	Description
M2002	Authentication	
M2015	Cryptographic DSSS sequence	
M2003	Encryption of communications	
M2016	Frequency Hopping	
M2033	High-power up-link	
M2014	Spread Spectrum	
M2030	Usage of directive transmit antenna	

Thank You !

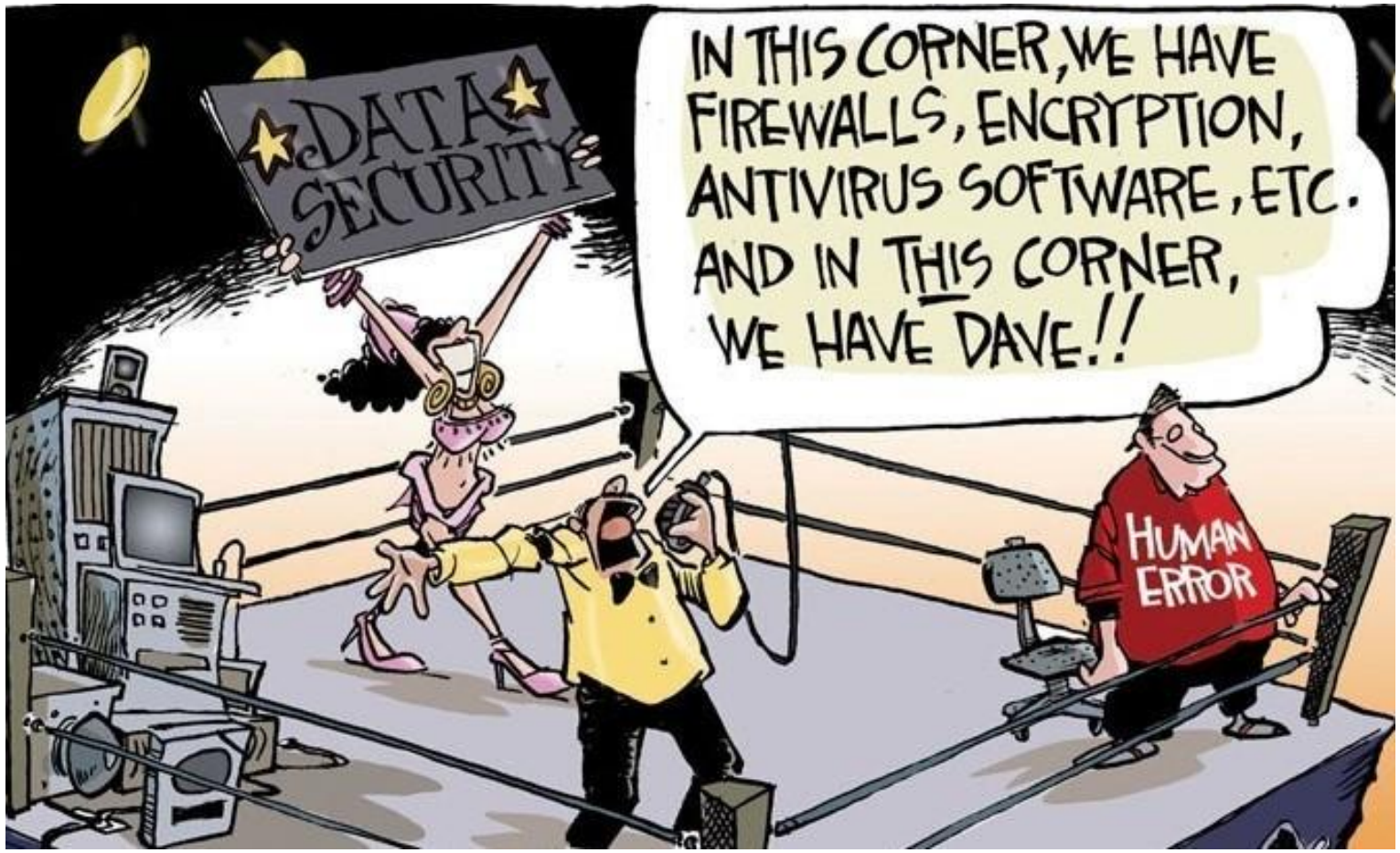


Image:strategicfocus.com

The evolution of standards and cybersecurity for NGSO satellite terminals

Mr. Marco MARCOVINA
Member of ETSI SES

ETSI

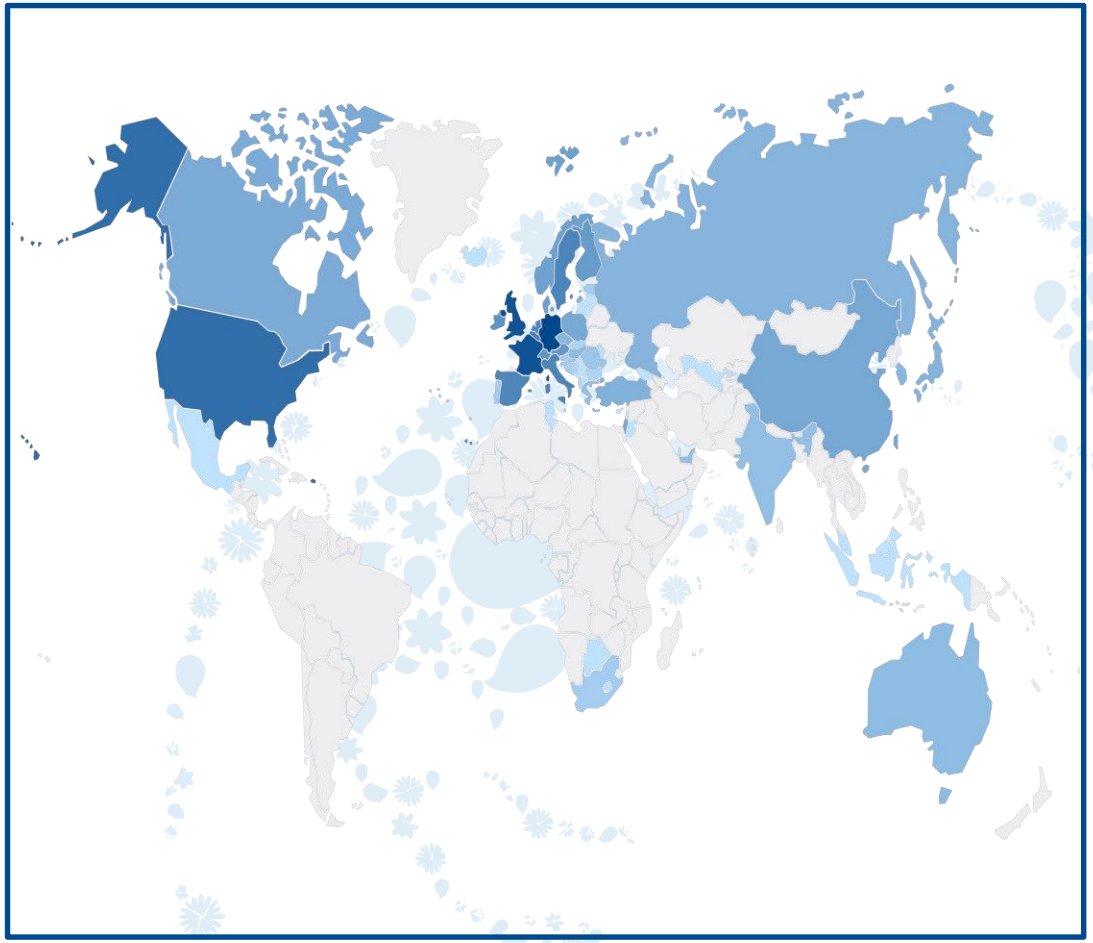
The Standards People

Agenda

- ETSI and ETSI SES
- RED Directive and CE marking
- Regulatory requirements (EU)
- Cybersecurity and satellite terminals in ETSI
- NGSO constellations
- NGSO constellations and cyber security
- ETSI standards for NGSO terminals
- Satellite communications and lawful interception in ETSI

ETSI and ETSI SES

- ETSI is a European Standards Organization (ESO). It the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. Supports European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).
- ETSI SES is responsible for standardization relating to all types of satellite communication systems, services and applications including fixed, mobile and broadcasting; satellite navigation systems and services; all types of earth stations and earth station equipment, especially the radio frequency interfaces and network and/or user interfaces; and protocols implemented in earth stations and satellite systems.



RED Directive and CE marking

- The radio equipment directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market.
- Gives essential requirements on: safety and health, electromagnetic compatibility, the efficient use of the radio spectrum and now cyber security.
- Compliance with the RED directive is a prerequisite for placing on the market and is testified by the CE marking
- The CE marking can be obtained via self-certification (if compliance with an harmonized standard cited in the OJ) or via a notified body

Regulatory requirements (EU)

In 2022 Article 3.3 (essential requirements) of the RED directive has been amended to cover cyber-security:

- Article 3.3(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service
- Article 3.3(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and the subscriber are protected
- Article 3.3(f) radio equipment supports certain features ensuring protection from fraud

Cyber security and satellite terminals in ETSI

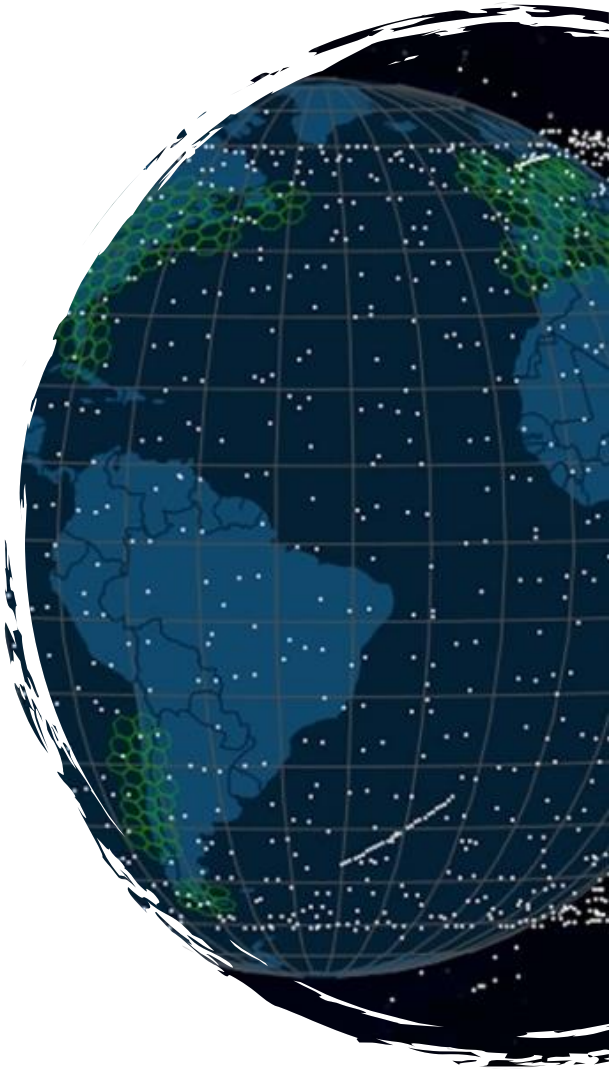
- EN 303 645 is not specific to satellite terminals, but it has been suggested to use as a reference for the CE marking process
- There is no ETSI standard for cybersecurity of satellites earth stations
- The current standards are developed in ETSI SES and mostly cover spectrum matters

EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements

- No Universal Passwords
- Mean to manage report of vulnerabilities
- Keep software updated
- Securely store sensitive parameters
- Communicate securely
- Minimize exposed attackedd surfaces
- Ensure software integrity
- Secure personal data
- Make system resilient to outages
- Examine system telemetry data
- Make simple for users to delete data
- Make installation and maintenance of devices easy
- Validate input data

NGSO Constellations

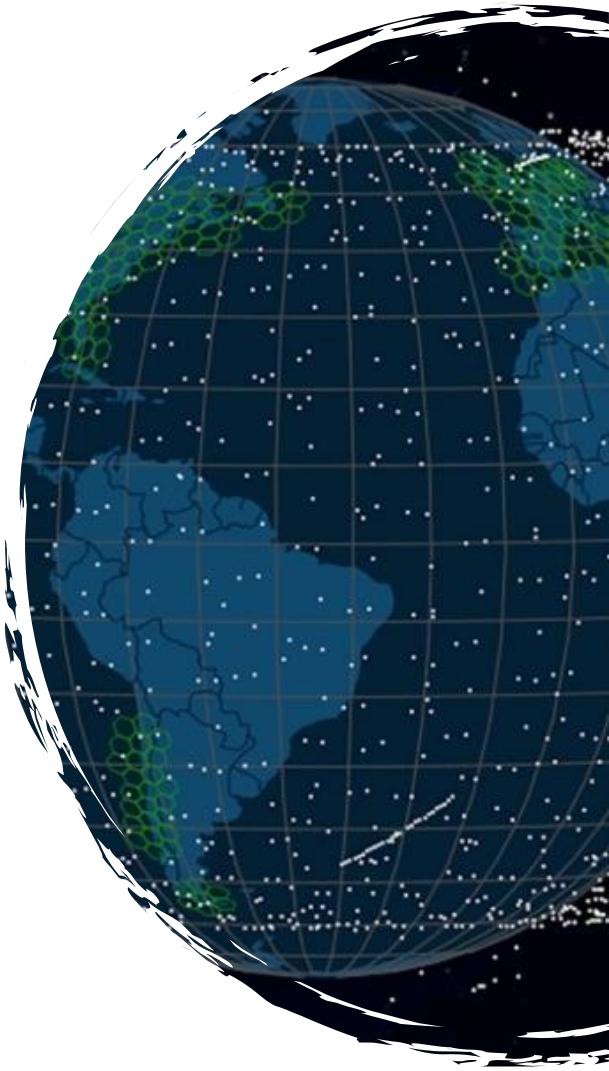
- Low Earth Orbit, non –geostationary constellations
- Orbit ranges from 500 to 800 km typically
- High capacity delivered by up to several thousands of multi-beam constellations
- Bit rate from hundreds of Mb/s, to GBp/s
- Low latency (tens of ms vs 500 ms)



NGSO constellations and cyber security

Specific additional aspects of a sat network w.r.t other networks:

- Security of the mission (prevent access to satellite and ground infrastructure), i.e. attack on satellite control, or payload
- Security of terminals (prevent improper use of terminals)
- Non-spoofable localization of the terminals
- Requirements on geo-fencing



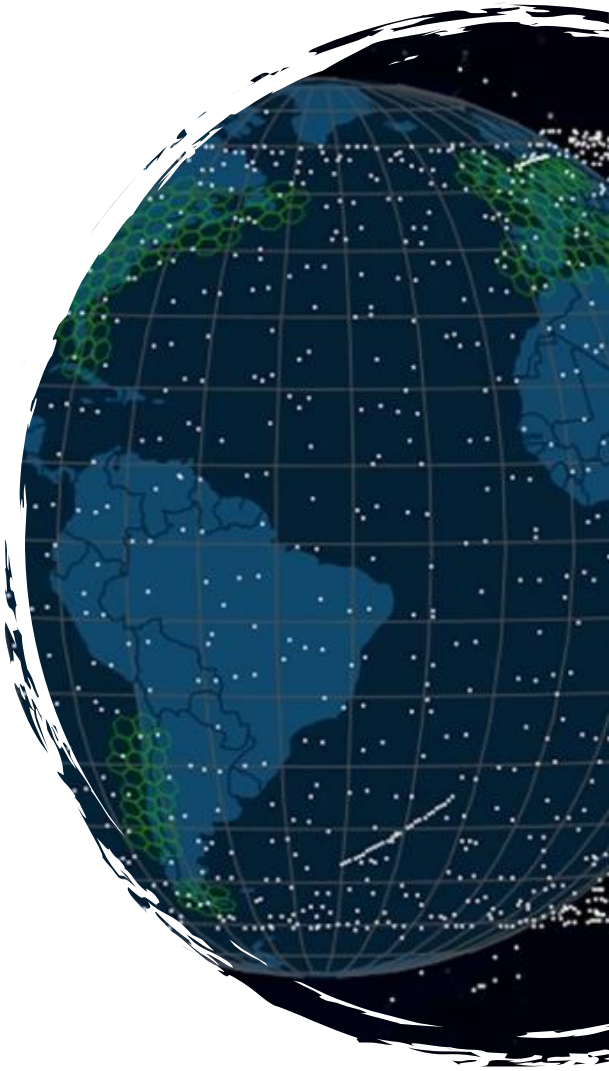
ETSI standards for NGSO terminals

Standards for terminals (ETSI SES purview):

- EN 303 699 (Ka, fixed)
- EN 303 979 (Ka, mobile)
- EN 303 980 (Ku, fixed mobile)
- EN 303 981 (Ku, fixed, mobile)

Standards for cyber security (ETSI CYBER purview):

- Currently there is no dedicated standard
- EN 303 645 (cyber security for IoT devices) can be used as reference by notified bodies
- CENELEC received a standardization request by the EC



ETSI SES discussed the matter of inserting requirements on cyber security in current standards, but the approach would rather be to have separate standards, likely by ETSI CYBER, in the same way of standards for EMC, with one general standard, and specializations for some cases where needed

Thank you for your attention

Follow us on:

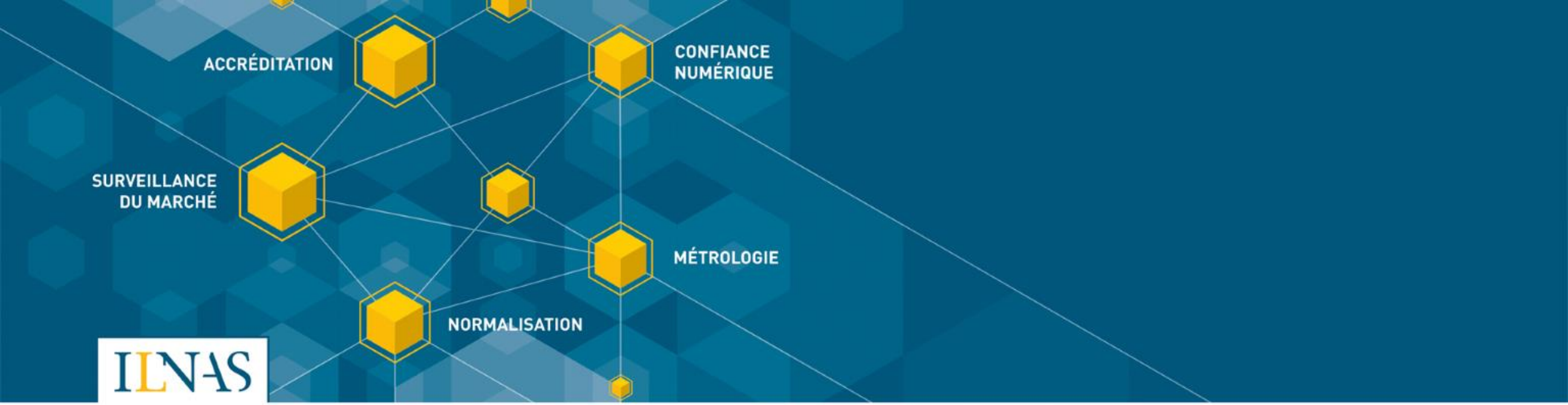
Any further questions?

Contact me:

mmmarcov@amazon.lu

Presentation of the June 2023 edition of the Standards Analysis Space Sector - Luxembourg

Dr. Lucas CICERO
Aerospace and Technical Standardization
Project Officer -ILNAS/OLN

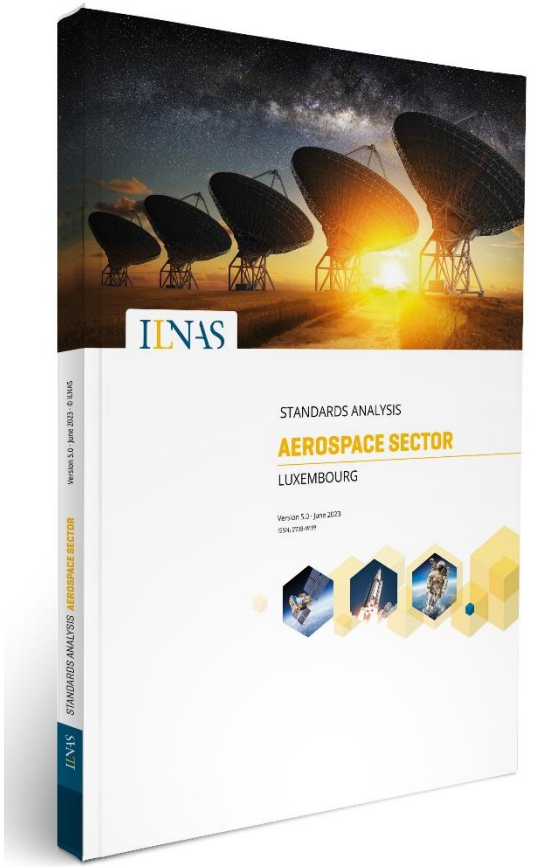


Workshop – Technical Standardization in Space and Cybersecurity

Presentation of the June 2023 edition of the
Standards Analysis Space Sector

27th June 2023

Dr. Lucas CICERO – Aerospace and Technical Standardization Project Officer, ILNAS/OLN



Main information

The importance of technical standardization in the Aerospace sector

Purpose

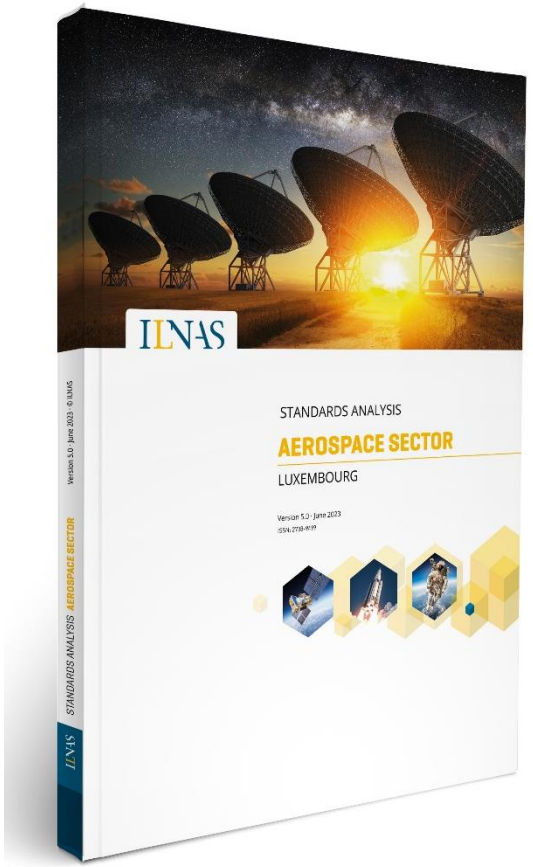
To help you identify :

- Relevant technical committees related to the Aerospace sector
- Relevant standards and projects addressing the Aerospace sector

What aims?

- Sources of technical standards that might impact/help you
- Understand the importance of technical standardization in Aerospace sector
- Identify standards development connected to your business in which participating in their development could be of interest

1. Content



Part 1

Introduction to the Aerospace sector

- Aerospace overview
- Aerospace market economy

Part 2

Standardization in the field of Aerospace

- Standards organizations and standards development process
- The importance of technical standardization in the Aerospace sector

Part 3

Opportunity for the national market

- How can technical standardization benefit the national market?
- How to become a national delegate and the advantage to be one?

Part 4

Aerospace Sector standards watch

- List of relevant Technical Committees

Aerospace overview

Europe

- Political guidance
- Funding programs and projects
- Entities

Luxembourg

- Aerospace policy and partnership
- Legal framework
- Entities

Aerospace market economy

Dynamic development areas

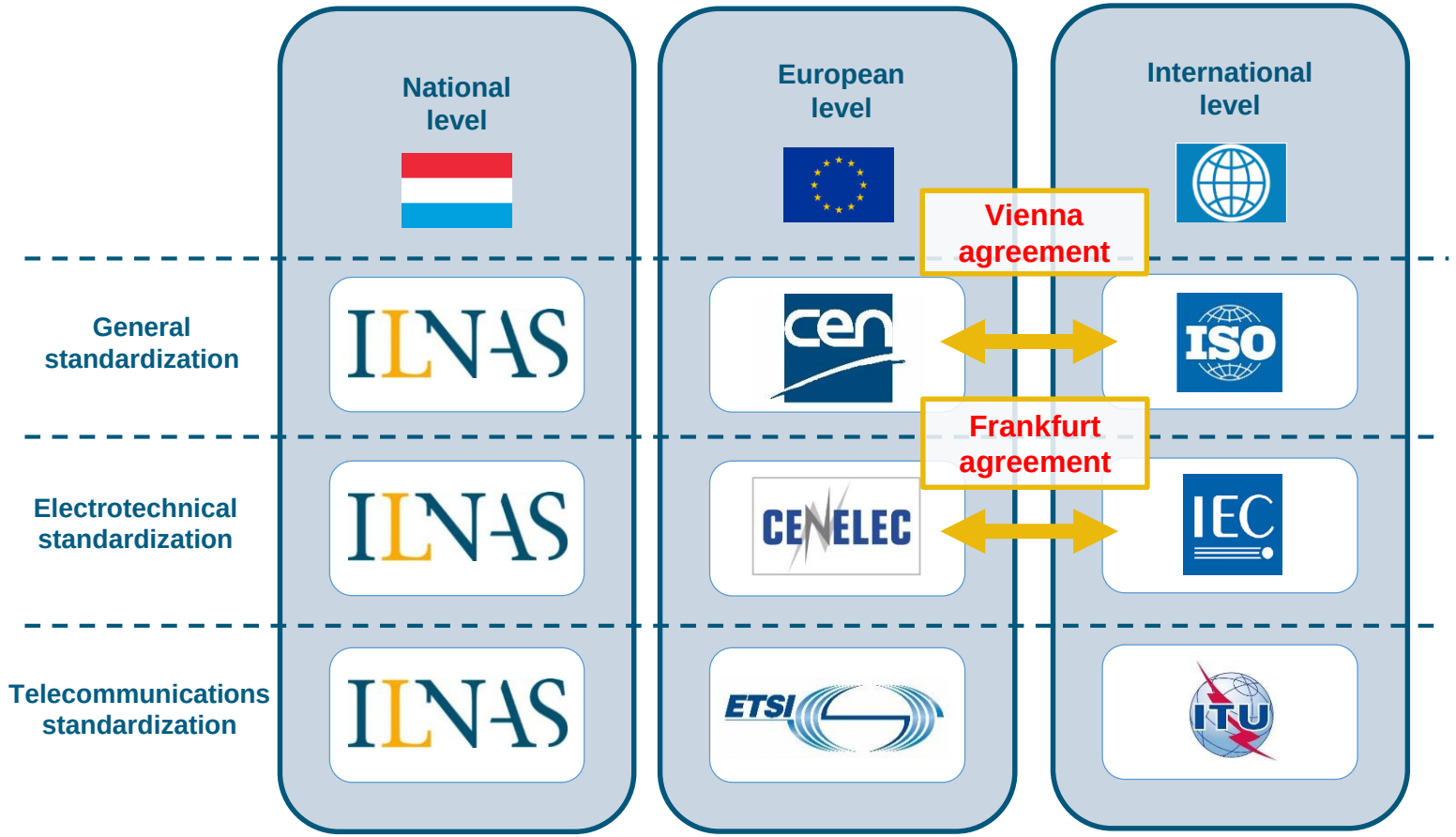
- Telecommunications
- Earth Observation
- Satellite Navigation

Promising development areas

- Space debris
- Space tourism
- Small satellite launch services
- Information and Communication Technology (ICT)
- Space resources
- Cybersecurity

Standards organizations and standards development process

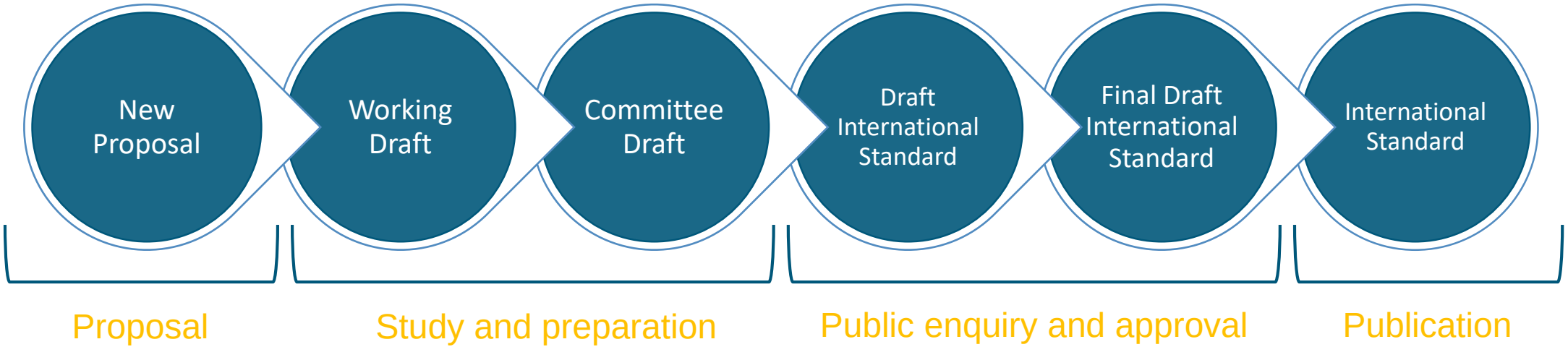
Standardization organizations



Standards organizations and standards development process

Standards development process

- Openness
- Impartiality
- Consensus
- Effectiveness and relevance



The importance of technical standardization in the Aerospace sector

Technical Standardization

- **Facilitate international collaboration** through the integration of products and services

- **Facilitate the interoperability of products**, to reduce the technical barriers between the different stakeholders and to facilitate the interface of systems

- Provide a set of guidelines and good practices that will **increase efficiency, reduce costs and improve quality**

How can technical standardization benefit the national market?

Which benefits?

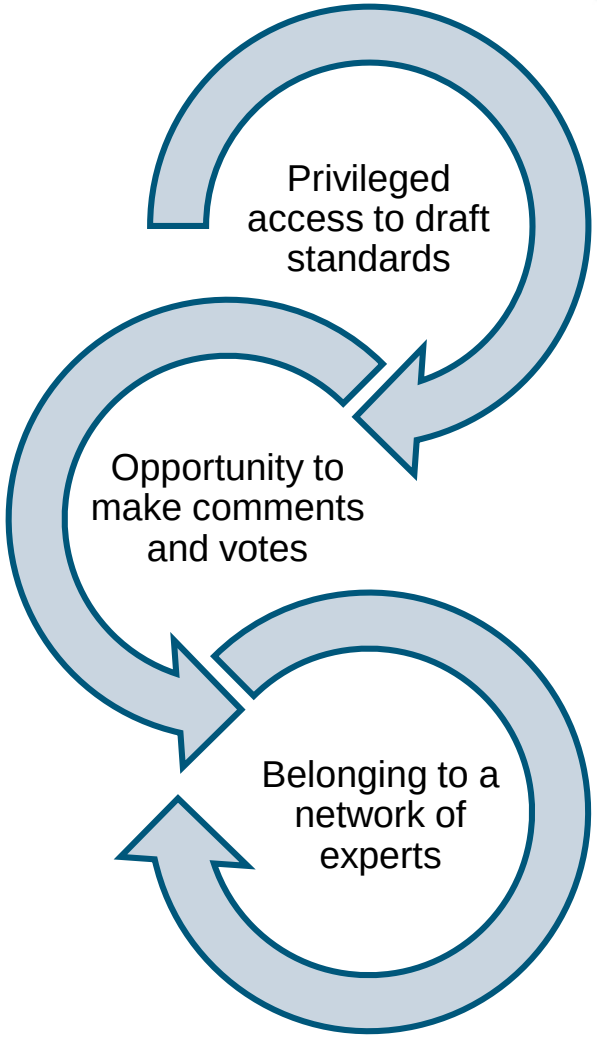
"an inclusive tool for performance and excellence to serve the economy"

- National market can **benefit from the definition of the future market rules.**
- The **common ground** provided by technical standardization is essential in the Aerospace sector as external cooperation is almost always involved. It can **extend the market and increase the number of partnerships.**
- Technical standardization is meant to **facilitate cooperation and reduce technical barriers** between the different stakeholders by promoting interoperability and the use of common interfaces.
- This increases the standards of **quality, security and transparency** of your company.

How to become a national delegate and the advantage to be one?

Why get involved in standards development?

- Access drafts standards and influence their content based on your know-how
- Learn about your competitors and their positions in meetings
- Promote your organization and your skills at national, European and international levels
- Propose new standards projects
- Increase your knowledge regarding the state of the art in standardization of your core business
- Anticipate the evolution of your activity sector's good practices
- Integrate strategic network of national, European or international experts
- Collaborate to defend common interests



How to become a national delegate and the advantage to be one?

Becoming a delegate

- **What are the tasks?**

  Technical support for standard development activities

  Provide your expert's view in WG votes

  Be part of the different development meeting

  Provide your position at International Technical Committee

- **Who can participate?**

  Every socio-economic actor in Luxembourg with a certain expertise

- **Costs: just time**

  The participation in Luxembourg is free of charge

- **How to register?**

  Your can apply to become a national delegate in standardization by completing the registration form "ILNAS/OLN/F001a" (Initial registration) or "ILNAS/OLN/F001b" (Additional registration)*

List of relevant Technical committees

Regrouped into 5 parts:

- Solely dedicated to the space sector, with a wide range of applications
- Telecommunications
- Earth Observation
- Technical areas (mechanical, electrical…)
- Systems engineering, Quality, Safety and Management processes

4 major technical committees:

- ISO/TC 20/SC 14 “Space systems and operations”
- CEN/CLC/JTC 5 “Space”
- ASD-STAN “Aerospace”
- ETSI/TC SES “Satellite Earth Stations and Systems”

Technical Committees

ISO/TC 20/SC 14 Space systems and operations			
GENERAL INFORMATION			
Creation date	1992	Secretariat	ANSI (United States)
Chairperson	Mr Frederick Slane	Committee Manager	Mr. Nick Tongson
Scope	Standardization for manned and unmanned space vehicles, their design, production, testing, integration, maintenance, operation, and disposal, and the environment in which they operate, as well as the safety requirements associated.		
Structure	AG 1 Chairman's advisory group (CAG) AG 2 Terminology task force WG 1 Design engineering and production WG 2 System requirements, verification and validation, interfaces, integration, and test WG 3 Operations and support systems WG 4 Space environment (natural and artificial) WG 5 Space System Program Management and Quality WG 6 Materials and processes WG 7 Orbital Debris Working Group WG8 Downstream space services and space-based applications		
Webpage	https://www.iso.org/committee/46614.html		
STANDARDIZATION WORK			
Published standards	190	Projects	47
INTERNATIONAL MEMBERS			
P-Members	16	O-Members	11 (including **Luxembourg**)

Technical Committees

Non-exhaustive list of current activities:

- **CEN/CLC/JTC 5** – Space
  - *ECSS adaptation to CEN/CENELEC in context of standardization mandate from EC*

- **ETSI/TC SES** – Satellite Earth Stations and Systems
  - *ETSI EN 303 979 -* ***Harmonised Standard for Earth Stations on Mobile Platforms (ESOMP) transmitting towards satellites in non-geostationary orbit, operating in the 27,5 GHz to 29,1 GHz and 29,5 GHz to 30,0 GHz frequency bands covering the essential requirements of article 3.2 of the Directive 2014/53/EU***

- **ISO/TC 20/SC 14** – Space systems and operations
  - *ISO/TS 6434 -* ***Space systems — Design, testing and operation of a large constellation of spacecraft***
  - *ISO/AWI 17770 -* ***Space systems — Cube satellites (CubeSats)***
  - *ISO/CD 9490 -* ***Space systems - Space Traffic Coordination***

ILNAS offers the following products and services to national socio-economic actors:

- **Dissemination of normative information**
  - Sectoral Standards Analyses (Fundamental Sectors)
  - Meetings
  - White papers
  - Newsletters
  - Etc.

- **Continuous training in standardization**

- **Targeted standards watch**

Main takeaways of the Aerospace Standard Analysis

Know the importance of technical standardization in the Aerospace sector

- Know some existing technical committees
- Know who is developing standards that might impact/help you
- Follow committees' work and standards' evolution
- Join as a delegate to
  - Shape new standards that are in project form
  - Rework published standards that are under revision
  - Propose new standards and lead projects

Know what services ILNAS can offer to support you

- Coach you as a delegate
- Serve as an interface to submit comments
- Propose standards watch

DON'T HESITATE TO:

- DIVE INTO THE DOCUMENT!
- CONTACT US!

Thank you for your attention!

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail: info@ilnas.etat.lu
www.portail-qualite.lu

Round table: Cybersecurity in the Luxembourg space ecosystem

Luxembourg Space Agency (LSA)
Mr. Charles KOENER - Policy Officer - LSA

Luxembourg House of Cybersecurity (LHC)
Mr. Pascal STEICHEN - CEO - LHC

National Standardization Commission 01 “Cybersecurity” (NSC 01)
Dr. Carlo HARPES - Managing Director - itrust consulting
Vice-President of NSC 01

University of Luxembourg
Dr. Grégoire DANOY - Deputy-Head of the Parallel Computing and Optimisation Group (PCOG)
Ms. Maria HARTMANN - PhD student - University of Luxembourg