Council of the
European Union

Brussels, 19 February 2024
(OR. en)

6767/24

ESPACE 16
INTER-REP 15

COVER NOTE

Subject:	Presentation of the European Space Policy Institute's activities and of the main takeaways of the Presidency's workshop on cyber resilience in space and key aspects of ESPI's recent report on "space, cyber and defense" - Powerpoint presentation (Space WP meeting 19.02.2024)

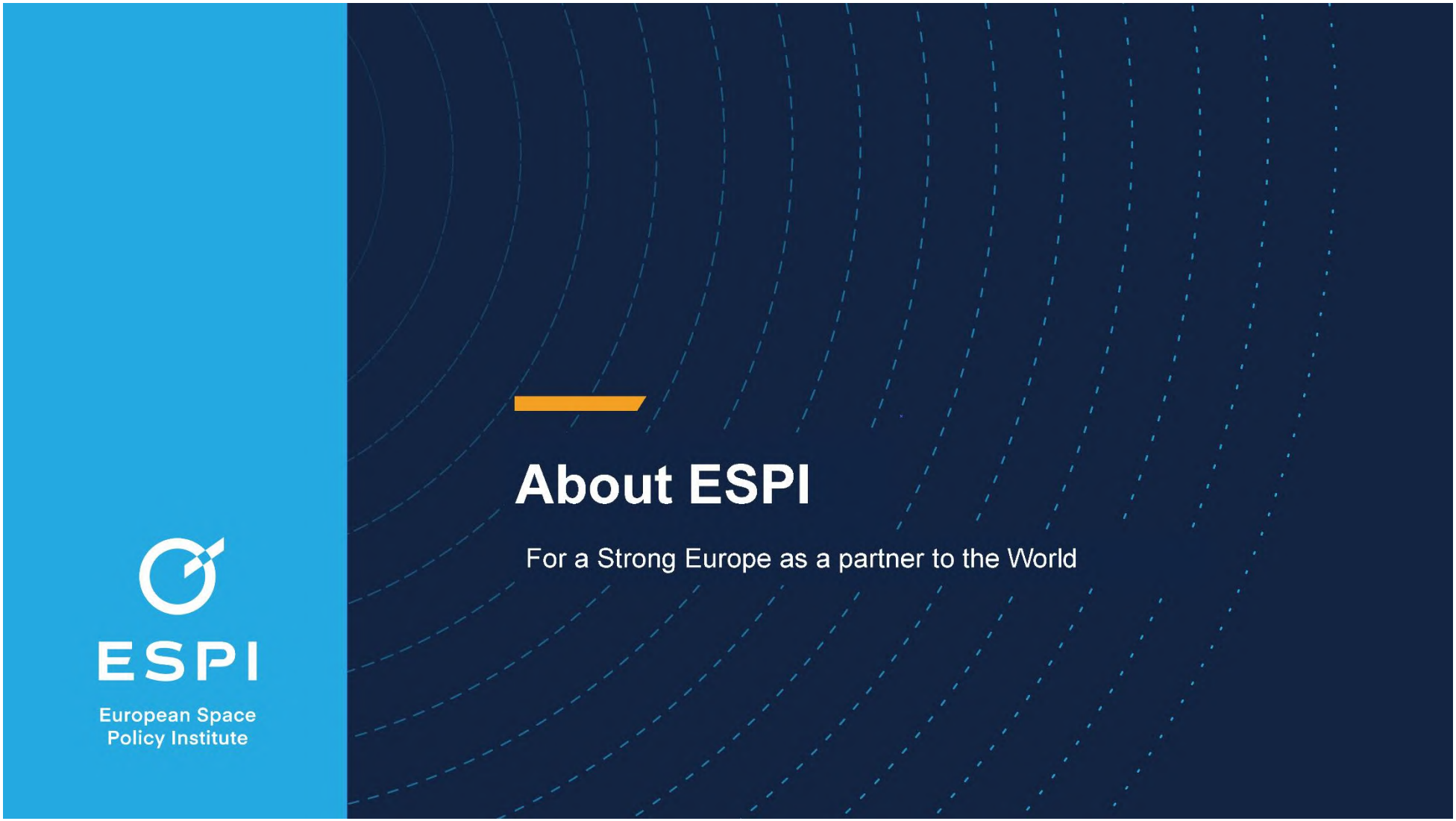
This document contains a presentation by an external stakeholder and the views expressed therein are solely those of the third party it originates from. This document cannot be regarded as stating an official position of the Council. It does not reflect the views of the Council or of its members.

ESPI

European Space Policy Institute

ESPI presentation at EU Council's Working Party on Space, 19 Feb 2024

Tomas Hrozensky, *tomas.hrozensky@espi.or.at*
Clémence Poirier, *clemence.poirier @espi.or.at*


ESPI
European Space
Policy Institute
About ESPI
For a Strong Europe as a partner to the World

ESPI Mission and Agenda

ESPI European Space Policy Institute

ESPI is Europe's independent think tank for space based in Vienna, Austria – the world's capital of space diplomacy. Working in a non-profit capacity, ESPI:

- **Promotes European space policy on a global level;**
- **Facilitates an active forum for the analysis and discussion of European needs, capabilities, and long-term prospects in space activities;**
- **Develops approaches to European space policy;**
- **Makes proposals and recommendations to European decision-makers and**

ESPI's mission is implemented through the ESPI Agenda, which is comprised of three types of activities: **European and International Engagement**, **Research**, and **Education**.

ESPI Governance and People

ESPI European Space Policy Institute

Co-founder *Co-founder*

FFG · esa · arianespace · belspo · beyond gravity · European Commission

EUMETSAT · EUTELSAT GROUP · EXO LAUNCH · DLR · asi

LUXEMBOURG SPACE AGENCY · cnes · Norsk Romsenter · OHB · AGÊNCIA ESPACIAL PORTUGUESA · rosa

ThalesAlenia Space · UK SPACE AGENCY · Supported by Federal Ministry Republic of Austria Climate Action, Environment, Energy, Mobility, Innovation and Technology

20 member organisations

Advisory Council

Interdisciplinary staff of 20+ nationalities

10 experts from across Europe's space sector (50% gender balance), currently chaired by:

Etienne Schneider
Chair, Former Deputy Prime Minister of Luxembourg

Research - ESPI's key publications in 2023

ESPI European Space Policy Institute

REPORTS

Space Venture Europe 2022

Safety & Sustainability Momentum

Space Spectrum Management

Space, Cybersecurity & Defence

Value of Space Exploration

WITH

esa BCG

Space & Civil Society

WITH

European Economic and Social Committee

Future of Space Exploration

WITH

COPENHAGEN INSTITUTE FOR FUTURES STUDIES

OSAM State of Play & Future

WITH

WAY 4 SPACE

ESPI2040

ESPI's Policy vision for Europe in Space

DIRECTORS PERSPECTIVES

(Monthly)

BRIEFS

SPACE SECTOR WATCH

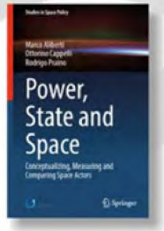
ESPI Insights

(Monthly)

ESPI Yearbook 2022

BOOKS

Power, State & Space



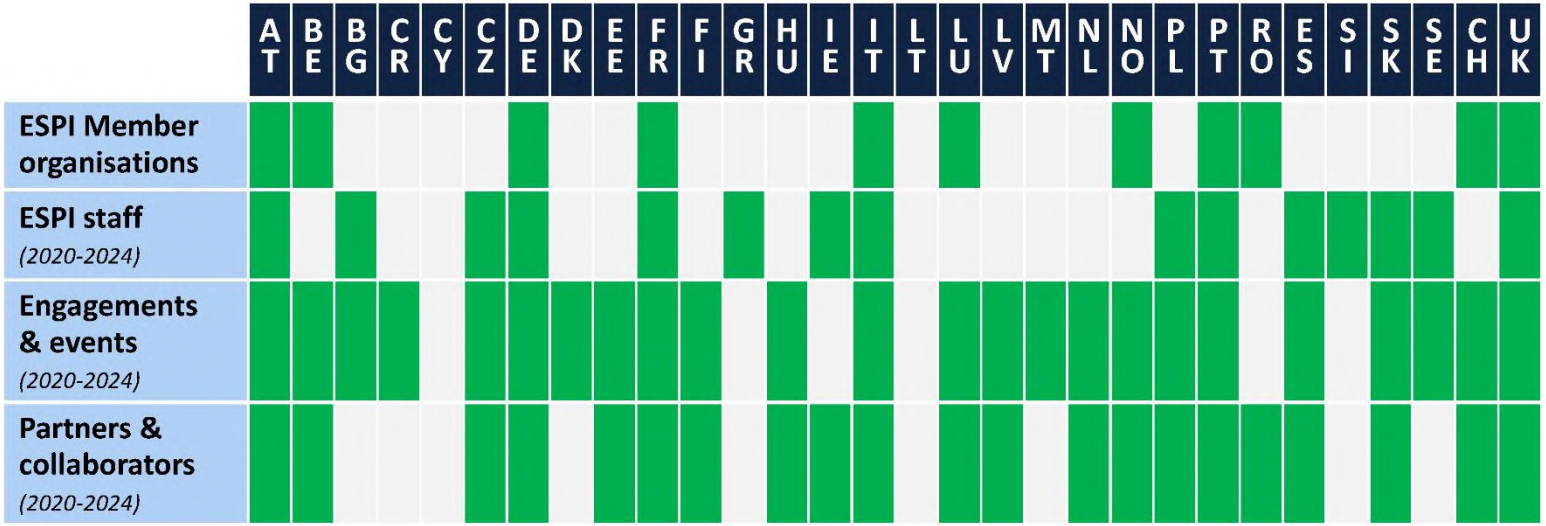
WRITTEN INPUTS TO POLICY-MAKING

- EU Space Strategy for Security & Defence
- EU Mid-Term Evaluation of the EU Space Programme
- EU Space Law

European and International Engagement

ESPI European Space Policy Institute

Presence across 30 EU and ESA member states



Global reach across seven continents

APRSAF ASIA-PACIFIC REGIONAL SPACE AGENCY FORUM

GRULAC

Flinders University

ITU

ASLI African Space Leadership Institute

Space Policy Institute THE GEORGE WASHINGTON UNIVERSITY

AEROSPACE

SECURE WORLD FOUNDATION

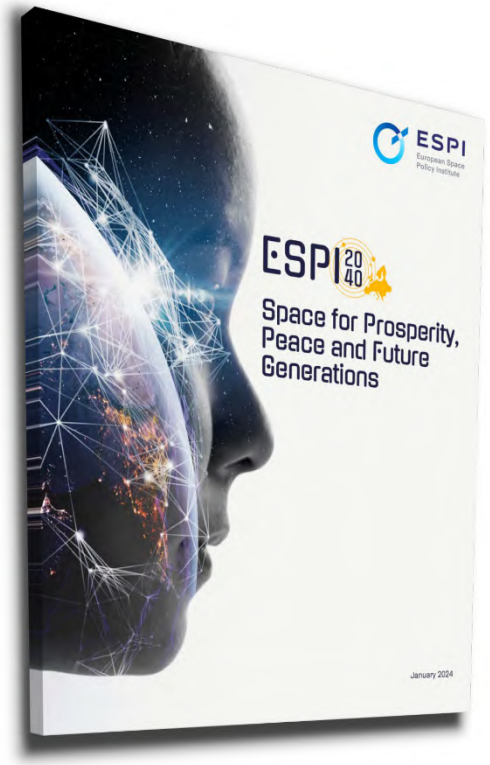
ORF OBSERVER RESEARCH FOUNDATION Ideas · Forums · Leadership · Impact

JAXA

KARI 한국항공우주연구원 KOREA AEROSPACE RESEARCH INSTITUTE

ESPI's 2040 Policy Vision for Europe in Space

ESPI European Space Policy Institute



Europe has all the prerequisites to develop into a full space power, by bringing together, federating and developing the excellence of its European, national and industrial capacities.

However, what is missing is a clear political will and a whole-of-Europe vision beyond the perceived bounds of space systems, which would precipitate policy impact.

To date, European space policy and programme action is mostly concerned with **space capabilities**, such as satellites and launchers, and less so with the **policy impact** of space. This includes how to integrate space into other policy sectors including security and defence, and how to build the required **foundations** in industrial competitiveness, scientific and technological excellence, innovation, talent and finance. Developing the policy impact of space is particularly critical at a time when crises affect policy priorities of public spending.

The *ESPI2040* Vision proposes to define and implement policy action on three levels and their interconnections:

ESPI

European Space Policy Institute

Key takeaways of the workshop of the Belgian Presidency of the Council of the EU

Cyber Resilience in Space

Panel 1: Current Landscape – Mapping Challenges

ESPI European Space Policy Institute

Space and cyberspace are recognized as warfighting domains.
Space is considered as a critical infrastructure since NIS2/CER Directive.

250 attacks recorded since the 1970s.
90 known attacks in 2023 alone.
30 attacks reported in January 2024 alone.
Low estimate as most attacks are not publicly disclosed.

Space systems include the space, ground, control and user segments.
Space companies and the supply chain are subject to cyberattacks.

Post-quantum cryptography and **physics-based encryption** methods.
Lack of standardization and demonstrated efficiency and robustness

Space companies **lack an understanding of applicable processes and reporting mechanisms** in case of cyberattack.

Proactivity is needed before a cyberattack happens. Security controls, cyber hygiene, standards, and intelligence sharing are needed to act beforehand.

EU Space ISAC to be created this year to share threat intelligence and best practices.
Governance and processes remains to be established.

Collaboration **within the space sector** and **across sectors** is essential

Panel 2: Future Strategies – Forging Resilience

ESPI European Space Policy Institute

Extraterritoriality: the law will apply to non-EU entities willing to do business in the EU
Proportionality based on the size and criticality of missions

EU space law should not jeopardise **competitiveness against non-EU entities** as well as **within the EU**

Adequate funding must be provided to ensure adherence and implementation by **SMEs and start-ups**

Cybersecurity can be costly; an attack can be devastating.
EU space law has to show that higher cybersecurity can become Europe's comparative advantage.

Cyber measures should not focus on specific technologies because technologies evolve and must interact with each other (QKD, PQE, etc.)

Technical requirements vary between countries. **Necessary to agree on minimum standards for cybersecurity**, including to obtain a license.

NIS2/CER Directive provide general rules but need to be **adapted to the space domain. Support to industries and agencies need to be given to implement the EU Space Law + NIS2**

Particular uses should be considered such as humanitarian operations to ensure **implementation of IHL** and **strictly segregate networks between civilian and military use**.


ESPI
European Space
Policy Institute
ESPI Expertise on Space
Cybersecurity

The War in Ukraine from a Space Cybersecurity Perspective

ESPI European Space Policy Institute

A case study of the KA-SAT cyberattack conducted by Russia a few hours before the invasion of Ukraine

Study conducted in August 2022

A self-funded study produced by ESPI

Analysis of cyber threats on the user segment and the space supply chain shows that the KA-SAT cyberattack is representative of the state of cybersecurity in the space sector

Analysis of the lessons to learn from this attack for the cybersecurity of the European space infrastructure

Final Report released in October 2022

ESPI Study – Space, Cyber and Defence

ESPI European Space Policy Institute

Investigation of the intersection between space, cyber and defence

Complexity of the space-cyber-defense nexus

Operational, legal, political and strategic implications of using commercial satellites in war

Analysis of the approach to space cybersecurity in the UK, France, and Italy

Collective Report
Call for papers to the space community

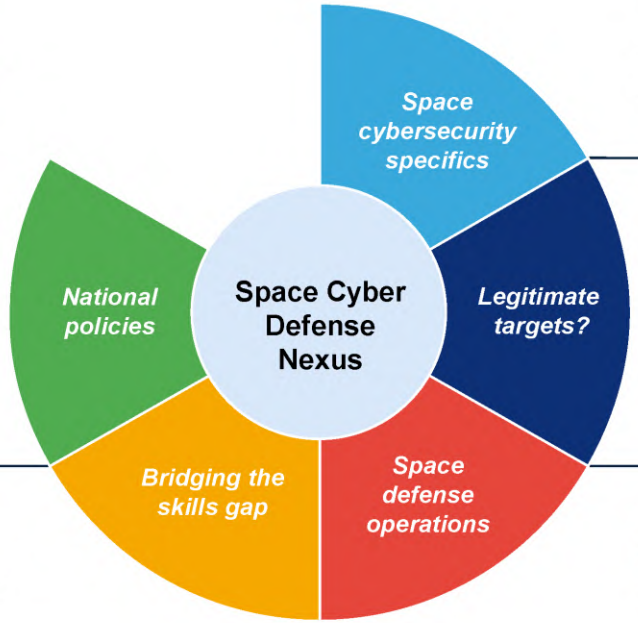
Final Report published in November 2023

Is cybersecurity in space the same as cybersecurity on Earth?

- On the ground, user, control segments, cybersecurity of space systems is similar
- On the space segment, cybersecurity is very different
- Challenges specific to the orbital environment

Heterogeneous national approaches to space cybersecurity

- No EU Member State has a dedicated strategy for space cybersecurity
- FRA, ITA, UK recognize cyber threats on space systems in space policies
- Only the UK recognize cyber threats on space systems in cyber policies
- Only the UK has cybersecurity obligations in national space law
- No single entity responsible for space cybersecurity



The nature of satellites: military, commercial, or dual?

- New situation with the provision of commercial services and not systems to belligerents
- Dual-use concept
- Renew the question of commercial assets as legitimate targets

Skills development, cyber ranges, space exercises, and wargaming

- Significant skills gap in space cybersecurity
- Need for more education and multidisciplinary efforts
- Resilience increases with exercises, cyber ranges, table top, and wargaming

Defining, conducting, attributing, and responding to an attack on a space system

- Uncertainties on the specific corpus of law that should be leveraged when conducting an attack in space
- Attribution is a complex task for cyberattacks
- When an action is clearly identified as an attack, is retaliation systematically allowed?