ERA LEARN

Funded by the European Union

ERA-LEARN Networking Event 2026

Bridging European Partnerships:

Connecting, Sharing, Growing

Tech Gate | Vienna

18 Nov. 2026

Parallel Workshop

A4 Resilient Partnerships

Preparing for crises and dealing with uncertainty through foresight, research security and strategic autonomy

Moderation: Michael Dinges, AIT

Agenda

Time	Activity
10:30–10:35	Welcome and introduction
10:35–10:45	Opening input: Foresight in times of crisis: lessons and insights from three workshops with the European Partnerships (Susanne Giesecke, AIT)
10:45–12:00	Three fishbowl discussion rounds: Anticipation, Response, Adaptation and learning
12:00–12:10	ERA-LEARN policy brief on research security and dual use, Self-Assessment Matrix (Severino Falcón Morales, AEI)
12:10–12:25	Open discussion of the policy brief and insights from the three rounds
12:25–12:30	Closing

ERA LEARN

Funded by the European Union

ERA-LEARN Networking Event 2026

Bridging European Partnerships:

Connecting, Sharing, Growing

Tech Gate | Vienna

18 Nov. 2026

Parallel Workshop

A4 Resilient Partnerships

Foresight in times of crisis: lessons and insights from workshops with the European Partnerships

Susanne Giesecke, AIT, Austrian Institute of Technology

Workshop set-up

- **Future-proofing Research and Innovation Strategies of European Partnerships**
  Participants explored how European Partnerships can prepare for an increasingly uncertain world and identified strategic action points to strengthen their resilience, adaptability and impact potential.
- **Three online cross-partnership foresight workshops**
  Each workshop was independent and followed a learning-by-doing approach. The results reflect contributions from individual participants and groups rather than a consensus position.

1 Trends & drivers	2 Framework scenarios	3 Cross-scenario comparison	4 Future-proofing strategy design	5 Plenary and discussion

3
workshops

72
participants

Two scenarios

- **Fractured Futures**
  A future characterised by limited cooperation, increasing fragmentation and uneven development.

- **Converging Horizons**
  A future characterised by strong cooperation, joint investment and sustainable, inclusive development.

The scenarios are not forecasts but two plausible visions of the future.

They served as a framework for reflecting on strategies under different future conditions and build on the Technology Partners FP10 Working Paper.

Trends and drivers

- **Geopolitics and economy**
  Declining multilateralism, concentration of strategic resources and technologies, supply chain disruptions and inequality.

- **Environment and resources**
  Circular shift and bioeconomy, future energy and sustainability, extreme weather events and natural resource shortages.

- **Technology and digitalisation**
  AI and data trust, physical-digital connectivity, cyber insecurity, quantum computing and synthetic biology.

- **Society and health**
  Societal polarisation, misinformation, skills shortages, increasingly complex societal challenges and health and well-being.

Participants started from a common set of pre-defined trends and drivers and selected those most relevant to their Partnerships.

Partnership resilience

- **Dependencies and value chains**
  Partnerships can reduce dependency on non-European technologies and strengthen European value chains where supply is highly concentrated.
- **Critical infrastructure and systems**
  Resilient infrastructure networks, monitoring systems, cyber resilience and climate resilience belong in research and innovation agendas.
- **Research security**
  Collaboration agreements need to address data sovereignty, export controls, dual-use aspects and political sensitivities.
- **Open cooperation**
  Scientific cooperation beyond Europe remains valuable where it brings relevant expertise, with engagement adjusted to strategic relevance and trust.

Resilience as a core capacity

Broader insights

- **Greater adaptability**
  Partnerships should anticipate change rather than respond to individual disruptions in isolation.
- **Stronger cross-partnership collaboration**
  Strategic cooperation across value chains builds resilient, cross-sectoral ecosystems.
- **More agile governance**
  Flexible funding and governance approaches keep Partnerships effective under a wide range of future conditions.

Even a more cooperative future would not remove unequal capacities, new resistance mechanisms or the need for strategic choices.

Inputs to the discussion

Anticipation

Strategic intelligence
Cross-functional teams monitor geopolitical developments and identify risks early.

Dependency mapping
Partnerships map critical dependencies and share knowledge on vulnerabilities.

Agenda updates
Regular SRIA updates integrate emerging technologies and societal developments.

Response

Rapid response mechanisms
Partnerships prepare for crises such as cyber attacks or spectrum shortages.

Crisis community
An informal crisis community supports exchange on health, pandemics and shortages.

Responsibility
Who decides on a change of direction, and are the right people prepared?

Adaptation and learning

Preventive action
Partnerships move from reactive responses towards long-term preparedness and anticipatory capacity.

Learning across Partnerships
Partnerships learn from those that are ending or more experienced.

Experimentation
Agile funding instruments create space to test new approaches.

Funded by the European Union

ERA-LEARN Networking Event 2026

Bridging European Partnerships:

Connecting, Sharing, Growing

Tech Gate | Vienna

18 Nov. 2026

Parallel Workshop

A4 Resilient Partnerships

ERA-LEARN policy brief on research security and dual use

Severino Falcón Morales, AEI

Policy brief at a glance

- International collaboration is in the DNA of Partnerships → different approaches, e.g. Chips JU vs Biodiversa+.
- Addressed to Partnerships, funding organisations, programme managers, research-performing organisations and policymakers involved in international cooperation.

1 Purpose

Geopolitical and technological shifts since 2022, and rules that keep changing while calls and projects run.

2 Three models

EU: openness with proportionate safeguards

US: research security within technological protection

China: innovation, self-reliance and national security

3 Implications for Partnerships

Partnerships rely on cross-national coordination. Responsibilities are scattered among the EU, MSs, RFOs and RPOs.

Collaboration-specific assessment, proportionate safeguards and clear roles across the research and innovation lifecycle.

4 Self-Assessment

Partnerships

Partnership calls

Partnership projects

Openness to international partners makes Partnerships both an asset and an exposure.

ERA LEARN

Funded by the European Union

Policy Brief on Research Security and Dual Use

- The policy brief compares 3 approaches: the EU, the US and China.
- It examines how differently these systems shape these concepts, and what those differences mean for international collaboration: participation conditions, access to knowledge and technology, shared responsibilities.

- No universally accepted definition of either **research security** or **dual use**

European Union

Research security is the overarching governance and risk-management framework.

Research security
Identify, assess and manage risks from international R&I cooperation.

Critical knowledge& technologies
Knowledge and technologies in emerging and strategic fields important for the EU 's competitiveness, welfare and security.
Includes, but is not limited to, R&I with dual-use potential.

Research with dual-use potential
Civilian research and innovation that could contribute to military, intelligence or other security-related capabilities.

Dual-use export controls
Legally controlled items, software and technology under Regulation (EU) 2021/821. Applies only when criteria are met.

Partial overlap: not all dual-use research is subject to export controls.

National security
Protection of the Union and its Member States, Union values and fundamental rights

United States

Research security and technology protection are key components of a broader national security strategy.

National security & technological leadership
Protect the nation, maintain strategic advantages and promote economic prosperity.

Interconnected pillars

Research security
Safeguard integrity of federally funded R &D; manage foreign influence and associated risks.

Protection of critical & emerging technologies
Identify and protect technologies critical to national security and economic leadership.

Export controls
Control export, re-export and transfer of items, software and technology (EAR/ITAR).

Investment screening
Review certain foreign investments for national security risks (CFIUS).

Industrial & innovation policy
Invest in and strengthen key sectors, supply chains and innovation.

Dual-use research & technologies
Civilian research and technologies with potential military, intelligence or other security applications. A cross-cutting concern across all pillars.

National security
Protect the United States and its citizens, institutions and way of life.

China

Research security is embedded in a unified system where dual use is addressed through civil–military integration and state-led control.

National security & national development
Safeguard sovereignty, ensure security and achieve national rejuvenation

Unified state system
Centralised leadership and coordination across government, industry, academia and the military.

Science & technology development
Advance key technologies and strategic sectors.

Civil–military integration (CMI)
Systematically integrate civilian and military capabilities.

Technology protection & control
Manage security risks, data and technology flows, including dual-use export controls.

Talent & ideas management
Mobilise and direct talent, knowledge and resources.

Dual-use applications via civil –military integration
Research and innovation outcomes are expected to serve both economic development and national defence when appropriate

National security
Protect the state, maintain stability and achieve long-term national goals.

Implications for international collaboration

Key ideas

Follow the principle “as open as possible, as closed as necessary”.

- **Each collaboration has a distinct risk profile**
  Exposure arises where sensitive knowledge, affiliated partners, access to data or infrastructure and a pathway to application come together in one project.
- **Assess the risks early on**
  Vulnerabilities often arise early, before actual risk identification even starts, such as through people, data, tacit know-how and access to infrastructure.
- **Consider hard constraints**
  Eligibility restrictions, sanctions and export controls provide broader boundaries but do not equal sufficient research security risk identification with regard to the specific context.

Key ideas

- **Differentiated burdens create unequal exposures**
  Each national funder checks according to its own rules, but in the case of low national guardrails, this can increase risks for all.

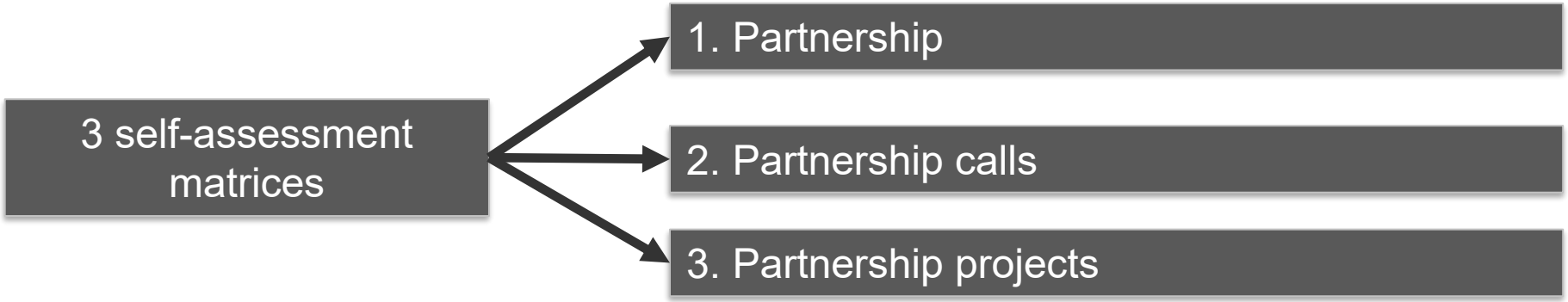
- **Consider the cumulative impacts**
  Researcher mobility or technology transfer may be fine project by project yet create dependencies across a portfolio.

- **Rules change faster (than projects are developed)**
  Review points and update clauses can be used to keep safeguards current without broader renegotiation.

Self-assessment - checklist

- **Purpose**

  To support Partnerships in identifying potential research security and dual-use risks when designing calls, selecting projects, establishing international collaborations and monitoring funded activities involving third-country partners.



Sections

- Project & Technology
- Third-Country Context
- Foreign Partner

- Collaboration Arrangements
- Safeguards & Governance

- etc

ERA LEARN

Funded by the European Union

Link:

Partnership / project: Partnership example

Assessor / date: Example 1

View dashboard | Export answers (JSON) | Import answers | Print / Save PDF | Reset

The data stays in this browser session unless you export it. No information is sent to a server. Save your answers as JSON to continue later.

1. Project & Technology | 2. Third Country Context | 3. Foreign Partner | 4. Collaboration Arrangements | 5. Safeguards & Governance | ★ Dashboard

Assessment dashboard

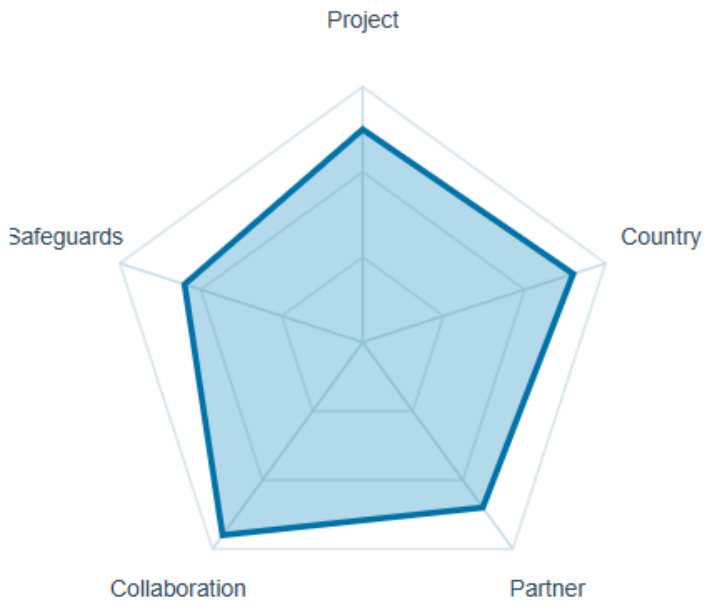
Partnership example · Example 1

26/27	14	1	0
Assessed criteria	High-concern criteria	Not applicable	Unanswered

Concern by dimension

Project & Technology	2.50 / 3
Country Context	2.60 / 3
Foreign Partner	2.40 / 3
Collaboration Arrangements	2.80 / 3
Safeguards & Governance	2.20 / 3

Risk profile



Priority issues and recommen

High Critical technology
Apply enhanced risk assessment where rele

High Sensitive research data
Develop a secure data management plan.

High Strategic relevance
Consider additional safeguards before disse

High Governance and rights framewor
Consider the broader cooperation context d

High Civil–military integration
Apply enhanced due diligence.

High Strategic dependencies
Assess alternatives and mitigation mea ures

High Sec y-rela d affiliations
Require enh ced r ew before approv l.

High Fundin nd affiliations
Request disclosure of funding and affiliations.

High Researcher exchanges
Establish access and travel security procedur

High Data and know-how
Establish secure information-sharing protocol

High Dissemination
Introduce proportionate publication review pr

DRAFT

Thank you

- **Foresight report and policy brief**
  Watch the ERA-LEARN newsletter for publications.
- **Get in touch**
  Share insights or suggestions on the two materials, or specific learning needs that ERA-LEARN could address.

Website:
www.era-learn.eu

Email:
office@era-learn.eu