CEIAS
Central European Institute
of Asian Studies

# Improving research security capacity of higher education institutions in Central Europe

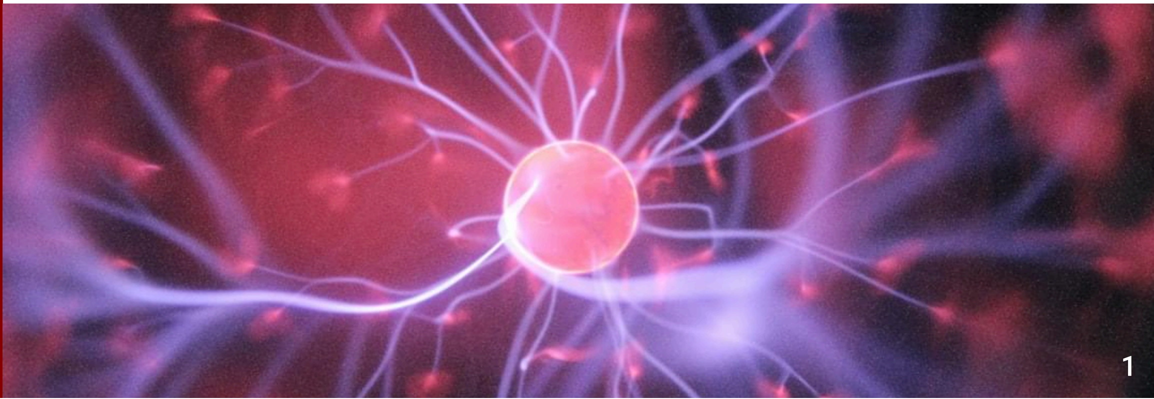
*Expert workshop summary*

**The imperative to strengthen research security within higher education institutions in Central Europe is underscored by the evolving landscape of international collaborations, particularly with entities from authoritarian countries (e.g., China and Russia).**

On March 12, 2024, CEIAS organized a workshop titled **Improving research security capacity of higher education institutions in Central Europe** on the sidelines of the 2024 CEEasia Forum conference.

The workshop gathered several international research and economic security experts, academic administrators, and policymakers in higher education to discuss the urgent need for research security in Central European higher education institutions.

This document presents the key takeaways from the discussion and recommendations for future action as understood by CEIAS.



# Executive summary

The imperative to **strengthen research security** within research institutions in Central Europe is underscored by the evolving landscape of international collaborations, particularly with **entities from authoritarian countries** like China. Recent discussions among experts and policymakers emphasize the **pressing need for robust policy measures** to safeguard research integrity and national security interests.

Research institutions face significant risks that warrant urgent attention. These risks include **transferring dual-use technologies** to adversarial beneficiaries**, industrial espionage**, or using research findings for **human rights abuses**.

To address these challenges, governments, research institutions, and individual researchers should follow below-outlined recommendations:

- **Research institutions should undertake comprehensive strategic reviews of partnerships, focusing on national security and ethical compatibility.**
- **In close dialogue with academic institutions, governments should develop policies prioritizing ethical standards and national security in international collaborations, ensuring transparency and adherence to human rights norms.**
- **Research institutions should strengthen the due diligence processes for vetting international collaborations.**
- **Relevant security agencies should implement comprehensive security awareness programs for all stakeholders involved in international research collaborations, focusing on identifying and mitigating potential threats.**
- **Governments should develop clear, stringent guidelines for conducting sensitive research safely and sustainably.**
- **All stakeholders should ensure that knowledge of and policies guiding research security are updated to keep pace with technological advancements.**
- **Research institutions should deploy comprehensive training programs on export control regulations and compliance. Research institutions should establish or strengthen institutional frameworks for export control compliance, including clear procedures and dedicated oversight bodies.**
- **Governments should incorporate the topic of research security into broader policies of economic security.**

# Scope of cooperation with Chinese entities in Slovakia and Central Europe

The technological sector, especially in the hard sciences, has been a focal point for Slovakia’s and Central Europe's academic cooperation with China. Such collaborations raise **critical concerns**, from **technology transfers** to **human rights implications** and the involvement with **entities linked to the People's Liberation Army**. Moreover, issues surrounding Confucius Institutes, contract transparency, and intellectual property rights signal areas warranting further scrutiny.

## Slovakia: Scope of academic cooperation with China

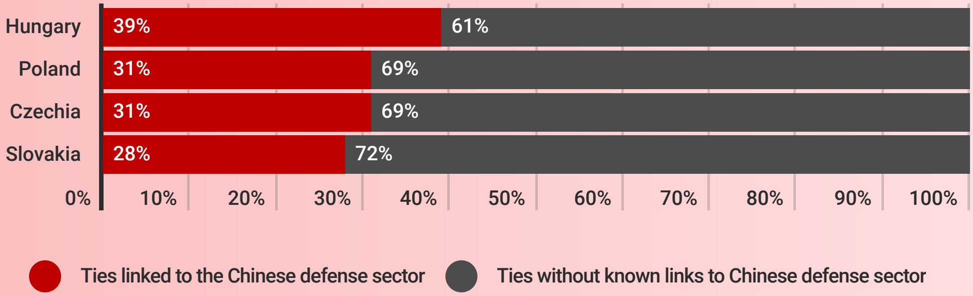
Previous CEIAS research, under the framework of the China-Europe Academic Engagement Tracker, identified **28 Slovak academic institutions** that maintain some link to Chinese partners. Altogether, these institutions have at least **136 connections to China**. Of these, 91 were entered into by Slovak public universities. The remaining 45 are tied to the Slovak Academy of Science and its various research institutes. Of the 136 academic interactions between Slovakia and China, **38 are with Chinese academic institutions tied to the People's Liberation Army**. Some 58% of these relations are with universities categorized by the ASPI Defense University Tracker as 'high risk' or 'very high risk.'

## Recommendations:

**Strategic review and risk assessment:** Research institutions should undertake a comprehensive strategic review of partnerships, focusing on national security and ethical compatibility, particularly scrutinizing collaborations with entities of concern.

**Policy development for ethical international academic cooperation:** In close dialogue with academic institutions, governments should develop policies prioritizing ethical standards and national security in international collaborations, ensuring transparency and adherence to human rights norms.

**Share of academic ties linked to the Chinese defense sector in the V4 countries:**



Data: China-Europe Academic Engagement Tracker

# Promoting research security agenda

The global research landscape's complexities necessitate a **fortified research security framework** that protects against intellectual compromise and operational vulnerabilities. Universities and academic institutions in Central Europe lack a comprehensive process and a body that promotes the agenda of research security.

Organizations such as the UK's Association of Research Managers and Administrators (ARMA) show the need for a sector-led intervention to enhance efficiency, equity, quality, and security in research collaborations. At the same time, such organizations provide a model that could be emulated to promote a bottom-up approach to research security.

**Lack of awareness** is a significant issue concerning research security, even in countries with the world's leading universities.

## Recommendations:

→ **Enhanced due diligence processes:** Research institutions should strengthen the due diligence processes for vetting international collaborations, incorporating standardized tools and questionnaires. Use examples from international success stories like that of ARMA in the UK.

*ARMA has produced several open-source resources, including a sample due diligence questionnaire. These materials are available on the **organization's website**. ARMA's report Complex Collaborations – Efficiency, Equity, Quality and Security in International Research provides more specific guidance for research managers. Additional resources were also developed by Universities UK.*

→ **Security education and awareness:** Relevant security agencies should implement comprehensive security awareness programs for all stakeholders involved in international research collaborations, focusing on identifying and mitigating potential threats. The impact of such programs can be multiplied by the involvement of think tanks active in the field or inter-university associations (e.g., Conference of Rectors or similar platforms).

# Weaponization of international research collaboration

**The potential misuse of academic collaborations by adversarial states for military or strategic gains poses a significant threat.**

Vulnerabilities of the academic sector are exacerbated by its inherent openness and internationalization as drivers of innovations.

Researchers tend to be blind to the potential security implications of their research or the collaborators they work with.

To be better equipped to identify potential risks and correctly implement mitigation measures, research security guidelines may help research institutions to navigate this problem area.

## Recommendations:

**Clear guidelines on sensitive research:** Governments should develop clear, stringent guidelines for conducting sensitive research safely and sustainably, ensuring robust vetting of projects and partners for security risks.

**Researcher education on sensitive areas:** Researchers involved in potentially sensitive research with knowledge that could be potentially misused by adversarial actors should be trained about relevant risks and the broader security context of their work. This should be done especially before engaging with higher-risk partners or traveling to higher-risk countries.

### A host of EU states and other partners adopted research security guidelines:

- **European Union:** *Council recommendation on enhancing research security (2024)*
- **European Union:** *Tackling R&I foreign interference (2023)*
- **Australia:** *Guidelines to counter foreign interference in the Australian university sector (2021)*
- **Czechia:** *Counter Foreign Interference Manual for the Czech Academic Sector (2021)*
- **USA:** *Recommended practices for strengthening the security and integrity of America's science and technology research enterprise (2021)*
- **Canada:** *National Security Guidelines for Research Partnerships (2021)*
- **United Kingdom:** *UK Research and Innovation - Trusted Research and Innovation Principles (2021)*
- **United Kingdom:** *Trusted Research Guidance for Academia (2023)*
- **Netherlands:** *National knowledge security guidelines (2022)*
- **Japan:** *Policy measures for ensuring research integrity in the global and open research environment (2021)*
- **South Korea:** *National R&D project security measures (2023)*

Note: This list is non-exhaustive.

# Evolving nature of dual-use technology framework

Rapid technological advancements necessitate a proactive and adaptive approach to managing the risks associated with dual-use technologies. Cutting-edge technologies are becoming increasingly dual-use, thus leading to a need for closer scrutiny and understanding. Authoritarian states, such as China, leverage AI to get a better hold of research that provides military and dual-use technology.

## Recommendations:

- **Regular policy and knowledge updates:** All stakeholders should ensure that knowledge of and policies guiding research security are updated to keep pace with technological advancements, emphasizing areas like AI, quantum computing, and other fields of cutting-edge advances.

- **Leverage AI technology for research security:** Researchers should use new technological developments, such as advances in AI, to create tools to strengthen research security. AI-based tools can provide a quick evaluation of potential dual-use applications of research outcomes and improve researchers' understanding of risk and needed mitigation measures.

| Priorities of Chinese research and development | | |
|---|---|---|
| Artificial intelligence | Quantum technology | Semiconductors |
| Neuroscience | BioTech | Clinical medicine |
| Deep space, deep sea, polar research | New materials | Major technical equipment |
| Robotics & smart manufacturing | Aerospace engines | Navigation systems |
| E-mobility | Medical equipment and pharmaceuticals | Agricultural machinery |

Adapted from: I. Karaskova et al. (2022): How to Do Trusted Research: China-Specific Guidelines for European Stakeholders.

# Improving capacities for export control

Robust export control mechanisms are critical for preventing the dissemination of sensitive technologies and information. Capacities for export control are lacking at Central European research institutions. Awareness of this area is often not deeply ingrained in research institutions. Changing regulatory frameworks often provide further issues for successful export control.

## Recommendations:

→ **Comprehensive training and tools:** Research institutions should develop and deploy comprehensive training programs focused on export control regulations and compliance, leveraging expertise from entities like the UK Higher Education Export Controls Association (HEECA). This will help to provide individuals from research institutions with tools they can leverage for a more efficient application of export control measures. Government agencies responsible for export controls should offer the necessary guidance to research institutions, especially when it comes to theimpacts of regulatory changes.

→ **Institutional compliance frameworks:** Research institutions should establish or strengthen institutional frameworks for export control compliance, including clear procedures and dedicated oversight bodies.

# Research security as economic security

Research security is inherently tied to economic security, as different country's strengths can be exploited. Taiwan's strategy to protect its semiconductor technology and R&D outcomes against foreign exploitation underlines this critical linkage. Taiwan's unique position concerning China and its semiconductor industry provides a case study on practical approaches to the research-economic security nexus that can provide Central European countries with further insights.

## Recommendations:

→ **Implement rigorous investment screening:** Governments should adopt stringent screening processes for foreign investments, particularly in sensitive technology sectors, to effectively identify and mitigate strategic risks. Such regulatory frameworks should also cover start-ups and spin-off companies that serve as bridges between academic research and its commercialization.

→ **Share lessons learned with like-minded partners:** Governments should engage in global partnerships to share strategies and best practices in protecting technological innovations, ensuring a harmonized stance against economic espionage and strategic exploitation.

# Promoting transparency of international research partnerships

The need for greater transparency in universities, especially regarding research security, is straightforward but often overlooked. Universities tend to be slow in sharing information with the public, with many of their contracts and collaborations not available online, leading to a lack of accountability. This lack of openness can hide potential conflicts of interest and security risks, undermining trust in academic institutions. Transparency in research collaborations ensures accountability and security and fosters trust within the academic community and with the public.

## Cooperation between Slovak and Chinese research institutions lacks transparency

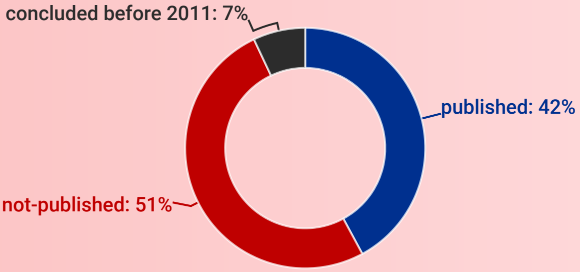
Since 2011, under the **Slovak Freedom of Information Act**, public institutions (including public universities and the Slovak Academy of Science) must **publish all the contracts** they enter into. Despite that, we identified that **less than half of the concluded cooperation contracts between Slovak research institutions and Chinese entities were made public**. Even when the agreements are published, the **disclosure quality is often problematic**. In the most extreme cases, contracts are redacted to such an extent that the disclosure fails to fulfill its purpose.

## Recommendations:

**Transparent reporting and documentation:**
Governments should mandate transparent reporting and documentation of international collaborations, making details accessible to the broader public. In cases where such reporting has already been implemented (such as in Slovakia or Czechia), compliance must be ensured.

**Engagement and dialogue:**
Open dialogue and engagement among stakeholders should be encouraged to discuss and address concerns related to research security. This includes stakeholders from the academic community, policymakers, and the public.

**Transparency of Slovakia-China research cooperation agreements:**



Data: China-Europe Academic Engagement Tracker

CEIAS
Central European Institute
of Asian Studies

This report was compiled by:

**Adam KALIVODA** | CEIAS Project Coordinator

✉ kalivoda@ceias.eu @AdamKalivoda

**Matej ŠIMALČÍK** | CEIAS Executive Director

✉ simalcik@ceias.eu @MatejSimalcik

**Published by:**
Central European Institute of Asian Studies
Murgašova 2, 811 04 Bratislava, Slovakia
www.ceias.eu
office@ceias.eu

**This publication and the associated event were organized and published in partnership with and support of:**

UK Science
& Innovation
Network