2026

10 KEY LESSONS ON RESEARCH SECURITY

10th Annual Seminar on Academic Security and Counter Exploitation (ASCE)

DMITRI TEPERIK

DR. SOLVITA DENISA-LIEPNIECE

10 Key Lessons from the 10th Annual Seminar

on Academic Security and Counter Exploitation (ASCE)

Dmitri Teperik and Dr. Solvita Denisa-Liepniece

Tallinn-Riga

2026

Authors:

Dmitri Teperik www.linkedin.com/in/dmitri-teperik

Dr. Solvita Denisa-Liepniece www.linkedin.com/in/solvita-denisa-liepniece-92587b197

This policy brief has been published within the framework of the Knowledge & Innovation Security Development Programme.

INTRODUCTION

The Annual Seminar on Academic Security and Counter Exploitation (ASCE) is a premier international gathering that brings together experts from government, academia, industry and the broader security community to discuss emerging risks facing the global research and innovation ecosystem. Hosted by Texas A&M University and the Security and Competitiveness Institute, the seminar provides a valuable platform for strategic dialogue, exchange of best practices, and the development of practical approaches to safeguarding research integrity and security while maintaining international scientific collaboration.

The 2026 seminar gathered more than 500 participants from 31 countries. The Baltic states were represented by Dr Solvita Denisa-Liepniece and Mr Dmitri Teperik[1], who also participated in the Sandia National Laboratories side event *"Securing the Future: Success Stories in Research Security Implementation"*, where regional challenges and opportunities for cooperation were discussed.[2]

Among the featured keynote speakers were Mr. Chris Raia (FBI Co-Deputy Director), Ms. Anna Puglisi (White House Office of Science and Technology Policy), Dr. Glenn Tiffert (Distinguished Research Fellow, Hoover Institution, Stanford University), Ms. Maria Cristina Russo (Deputy Director-General for Innovation, Prosperity and International Cooperation, European Commission), Dr. Kevin Gamache (Chief Research Security Officer, The Texas A&M University System), Dr. Beth Kolko (Director, SECURE Center, University of Washington), and Dr. Rebecca Spyke Keiser (Chief of Research Security Strategy and Policy, U.S. National Science Foundation). The programme also included prominent experts and practitioners from Canada, Australia, the United Kingdom, and other partner countries working on research security policy and implementation.

The key lessons outlined below summarise the main conclusions and insights that emerged from the keynote speeches, expert panels and side-event discussions held during the ASCE seminar.

[1] The authors previously published a study report entitled *'Enhancing Research Security in Latvia and Estonia: Potentials for Mitigating China-Related Risks in Academic Collaboration'*. See more: https://doi.org/10.13140/RG.2.2.12653.91360

[2] The authors would like to thank the team at Sandia National Laboratories, particularly Chris Cutrone and Michael Hollis, for their support in facilitating research security cooperation in the Baltics and for their participation in the ASCE 2026 conference.

1. Understand strategic science policies of authoritarian states

Effective research security requires a clear understanding of how authoritarian regimes and strategic competitors organise, fund, and direct their national research and innovation systems. For instance, China has further intensified the centralised management of science and technology development to accelerate every stage of the innovation chain — from basic research to applied technologies and industrial deployment. Similar state-directed approaches to research and technology development can also be observed in other strategic competitor states that integrate civilian and military research, allowing scientific advances to move rapidly into dual-use and military applications. Such policies are closely linked to broader national strategies aimed at achieving technological self-reliance, strengthening economic competitiveness, and expanding geopolitical influence. For research institutions in open democratic societies, this underscores the importance of strategic awareness when engaging in international collaboration. Understanding the policy frameworks, institutional structures, and long-term priorities of authoritarian regimes and competitor states helps researchers and decision-makers better assess potential risks and make informed choices about partnerships, knowledge sharing, and technology transfer.

2. Look beyond familiar scientific ecosystems

Research security risk assessments should not be limited to traditional indicators such as collaborations with well-known universities, publications in reputable journals, or participation in established academic networks. In an increasingly complex global environment, knowledge transfer and influence operations may occur through a much wider ecosystem of actors and organisational formats. Authoritarian states and strategic competitors often operate through indirect channels that appear benign or purely professional, making risks less visible to researchers and institutions. These channels may include non-governmental organisations,

government-organised NGOs (GONGOs), think tanks, industry associations, philanthropists, research foundations, and professional networks that facilitate exchanges, mobility programmes, conferences, and collaborative projects. While many of these organisations play legitimate roles in international cooperation, some may serve as intermediaries for strategic influence, technology acquisition, or agenda shaping. As a result, research institutions should adopt broader due diligence approaches that assess the wider institutional context of partnerships, funding sources, and collaborative platforms. Understanding these extended ecosystems helps identify hidden linkages and camouflaged patterns of influence, ensuring that decisions about cooperation are informed not only by scientific merit but also by a realistic assessment of strategic risks.

3. REVISIT THE DEFINITION OF FUNDAMENTAL RESEARCH

Rapid innovation cycles mean that even early-stage research can quickly acquire strategic, commercial, or dual-use (i.e. civil and military) relevance. Scientific discoveries that were previously considered purely theoretical may now be integrated into applied technologies within a short timeframe, particularly in fields such as artificial intelligence, advanced materials, quantum technologies, and biotechnology. This acceleration challenges the traditional understanding of "fundamental research" as inherently low-risk or open by default. As a result, research institutions and funding agencies need more nuanced frameworks for assessing risks associated with international collaboration, data sharing, and publication practices. Revisiting the definition of fundamental research does not imply restricting scientific openness, but rather ensuring that risk awareness and responsible decision-making are embedded throughout the research lifecycle. At the same time, research security discussions should not be limited to technological domains alone. Social sciences and humanities play an increasingly important role in strengthening cognitive security — the ability of societies to understand, anticipate, and resist influence operations targeting public perception, knowledge systems, decision-making and democratic institutions. Authoritarian regimes and strategic competitors have placed growing emphasis on shaping narratives, influencing

academic discourse, and studying foreign societies in order to gain ideological, informational, and psychological advantages. Concepts such as the Chinese strategic notion of the "colonisation of minds" illustrate how cognitive and informational domains are increasingly viewed as arenas of geopolitical competition. Strengthening expertise in social and humanitarian sciences is therefore essential for building resilience, improving strategic awareness, and supporting responsible decision-making within open research environments.

4. Universities and industry must actively manage security risks

Universities and industry today increasingly operate in a complex geopolitical environment where research collaborations, data access, and knowledge transfers can carry reputational, legal, and security implications. Incidents involving the leakage of sensitive data, misuse of research results, or undisclosed affiliations may not only undermine institutional credibility but also affect national research ecosystems and international partnerships. In order to address these risks effectively, universities and their industrial partners require clear governance structures, internal compliance mechanisms, and transparent procedures for identifying and managing risks and responding to incidents. Equally important is the establishment of trusted cooperation channels with government agencies, funding institutions, and security stakeholders. Such cooperation allows institutions to access relevant threat awareness, align with national security frameworks, and ensure that responses to potential incidents are coordinated, proportionate, and supportive of responsible scientific collaboration. Effective risk management also requires closer coordination across the broader research and innovation ecosystem, including technology transfer offices, start-ups, venture capital actors, and international research partners. Practical risk identification frameworks increasingly include structured screening questions regarding partner institutions, affiliations with restricted entities, participation in foreign talent recruitment programmes, and involvement in sensitive dual-use technologies.

5. Researchers as the front line of academic security: co-designing effective solutions

Researchers themselves are the primary actors within the research ecosystem and therefore represent the first line of defence in safeguarding knowledge, data, and innovation outcomes. Effective research security cannot rely solely on top-down compliance mechanisms or administrative procedures. Awareness, training, and individual responsibility at the researcher level are essential for recognising potential risks in international collaborations, data sharing practices, funding arrangements, and publication decisions. Researchers should also exercise professional prudence in everyday interactions and remain alert to elicitation techniques aimed at extracting sensitive information through informal conversations, networking events, or seemingly benign collaboration requests. As in every security domain, the human factor often remains the weakest link. At the same time, security measures are far more likely to be effective when they are co-designed with the research community. Human-centred design and engineering approaches help ensure that research security frameworks are practical, proportionate, and compatible with the realities of scientific work. By involving researchers in the development of policies, tools, and training programmes, institutions can improve usability, strengthen trust, and encourage broader adoption of responsible research security practices across disciplines.

6. Security should be built into research and innovation from the start

Research security is most effective when it is integrated into the design phase of research projects rather than introduced retrospectively. As research becomes more interdisciplinary, data-intensive, and globally interconnected, potential vulnerabilities may arise at multiple stages of the research lifecycle — from project planning and funding arrangements to data management, collaboration structures, and dissemination of results. Embedding security considerations at the outset allows

research teams and institutions to anticipate risks early and design appropriate safeguards without disrupting scientific work later on. This approach requires the development of structured risk assessment processes that accompany the formulation of research proposals and partnership agreements. Elements such as partner due diligence, data governance, intellectual property protection, and compliance with export control or sensitive technology regulations should be considered early in project development. By adopting a "security-by-design" mindset, research organisations can better balance openness and collaboration with responsible management of sensitive knowledge and emerging technologies.

7. MENTORSHIP STRENGTHENS RESEARCH SECURITY CULTURE

Developing a sustainable research security culture requires more than policies and compliance mechanisms; it also depends on the transfer of knowledge and practical experience within the research community, both domestically and internationally. Mentorship plays an important role in this process by helping early-career researchers understand how to navigate complex international collaboration environments, manage sensitive information responsibly, and recognise potential risks associated with partnerships, funding sources, and technology transfer. Dedicated Research Security Mentorship Programmes can provide structured guidance, peer learning opportunities, and access to experienced practitioners who have dealt with real-world research security challenges. They can also serve as channels for sharing relevant threat awareness and intelligence insights between institutions, enabling researchers to better understand emerging risks and adapt their practices accordingly. Mentorship initiatives can also help translate complex research security guidance into practical advice tailored to specific disciplines and research environments. Such programmes help build institutional capacity over time, strengthen awareness across disciplines, and foster a shared sense of responsibility for protecting research integrity while maintaining open and productive international scientific cooperation.

8. Trusted "clearing houses" are needed

Research security governance often involves complex regulatory frameworks, technical terminology, and evolving threat assessments that can be difficult for individual researchers or academic institutions to interpret and implement. In this context, trusted intermediary organisations or platforms — often referred to as "clearing houses" — can play an important role in translating policy guidance into practical, actionable recommendations for the research community. Such entities can facilitate communication and coordination between governments, academia, industry, and funding agencies. By consolidating expertise, providing due diligence support, sharing risk assessments, and developing training resources, clearing houses help reduce fragmentation and improve the usability of research security policies. Their role is particularly valuable in international research environments, where institutions must navigate different regulatory regimes while maintaining transparent and responsible scientific cooperation. The principal concern is not only the formal governance architecture within universities, but also the gaps that emerge at cross-sectoral intersections — between academia, the private sector, think tanks, media organisations, and other civil society actors. A resilient research security ecosystem must therefore extend beyond universities and align with broader principles of total defence, comprehensive security, and a whole-of-society approach.

9. Learn from international best practices

Research security challenges are increasingly transnational, as scientific collaboration, data flows, and innovation networks extend across borders. No single country or institution has a complete solution for managing these risks. Strengthening research security governance therefore requires learning from international best practices and exchanging experience across national systems. Comparative approaches can provide valuable insights into policy design, institutional structures, risk assessment methodologies, and effective awareness programmes. Regular exchanges among governments, research institutions, and

expert communities help identify practical solutions that can be adapted to different contexts. Such cooperation also promotes greater alignment of standards related to transparency, integrity, due diligence, and responsible collaboration. By sharing lessons learned and coordinating approaches where appropriate, countries can collectively strengthen the resilience of the global research and innovation ecosystem while preserving the openness that underpins scientific progress. Universities and research organisations can benefit from observing how peer institutions in other countries implement due diligence procedures, researcher training, and partnership screening mechanisms. International platforms, joint training initiatives, and policy dialogues can further support the exchange of experience and the development of shared approaches to research security.

10. Responsible openness and risk-aware cooperation

A central challenge in research security is maintaining a careful balance between openness, cooperation, and protection. Academic mobility, international collaboration, and science diplomacy have long been essential drivers of scientific progress, enabling the exchange of ideas, development of joint research initiatives, and strengthening of trust between societies. Open research environments attract global talent, accelerate innovation, and contribute to addressing complex global challenges that require international cooperation. At the same time, openness can create vulnerabilities that may be exploited for the undesirable transfer of knowledge and technology, infiltration and undue influence within research environments, espionage targeting sensitive research, or sabotage of research infrastructure and data systems. Particular attention is increasingly given to undisclosed affiliations, participation in foreign talent recruitment programmes, and hidden sources of research support that may create conflicts of interest or expose institutions to security risks. Responsible openness therefore requires integrating risk awareness into the everyday practices of research institutions without undermining the openness that enables scientific discovery. Managing these risks requires

proportionate safeguards that enhance awareness, due diligence, and institutional resilience while preserving academic freedom and responsible international collaboration — principles that remain fundamental to the advancement of science.

Conclusion

The lessons emerging from the ASCE discussions highlight a growing recognition that research security must evolve from isolated compliance measures toward a comprehensive ecosystem approach integrating governance, scientific practice, and strategic awareness. In an increasingly interconnected and competitive global research environment, safeguarding knowledge, technology, and innovation outcomes requires coordinated efforts across universities, industry, government institutions, and broader civil society actors. In this context, research security is not only a matter of institutional governance but also an important component of economic security, technological competitiveness, and the resilience of democratic societies.

Strengthening research security does not mean restricting scientific openness. Rather, it requires ensuring that international collaboration is pursued responsibly and with greater awareness of potential risks. Researchers, universities, industry partners, and policymakers therefore share collective responsibility for safeguarding knowledge and ensuring that scientific cooperation remains both open and secure. As research collaboration continues to expand globally and innovation cycles accelerate, developing mature research security cultures will become increasingly important for sustaining open and trustworthy scientific ecosystems. By integrating security-by-design principles, engaging researchers, strengthening institutional governance, and fostering international cooperation, research communities can build resilient ecosystems that protect academic integrity while preserving the openness that remains fundamental to scientific progress and democratic societies.

NATIONAL CENTRE OF DEFENCE & SECURITY AWARENESS

ESTONIA | KAITSEN.EE