Research and Innovation Series (RIS)

Growing Intersection between Research, Technological Development, and National Security

Webinar Series

Sep 2025 – Mar 2026

Institute for Security & Development Policy

Stockholm Center for Research and Innovation Security (SCRIS)

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

RESEARCH AND INNOVATION SERIES (RIS)

Growing Intersection between Research, Technological Development, and National Security

CONTEXTUAL BACKGROUND

The Institute for Security and Development Policy (ISDP), through its Stockholm Center for Research and Innovation Security (SCRIS), launched the Research and Innovation Series (RIS) as an online platform to examine the growing intersection between research, technological development, and national security in an increasingly complex geopolitical environment. The series brings together policymakers, researchers, and practitioners to assess how different countries are responding to emerging risks linked to dual-use technologies, foreign interference, intellectual property protection, and strategic technological competition.

The series included a sequence of thematic sessions focusing on Sweden, the United States (U.S.), Estonia, and the United Kingdom (UK). The inaugural session on September 9, 2025, featured Swedish perspectives, with contributions from Albin Gaunt of the Swedish Foundation for International Cooperation in Research and Higher Education (STINT) and Dr. Christina Wainikka of the Confederation of Swedish Enterprise, focusing on the implications of openness and internationalization in research. This was followed by a session on U.S. perspectives on January 28, 2026, with Anna Puglisi and Jeffrey Stoff, which examined the growing emphasis on risk-based approaches, dual-use technologies, and the strategic role of public funding.

A subsequent discussion on February 27, 2026, further assessed the effectiveness of U.S. research security policies, featuring Jeffrey Stoff, and LJ Eads, with a focus on institutional practices, collaboration risks, and policy implementation gaps. The fourth session on March 17, 2026, explored Estonia's experience in cybersecurity and digital resilience, presented by Siim Alatalu, highlighting a whole-of-society approach to managing digital vulnerabilities and hybrid threats. The fifth session on March 31, 2026, addressed the UK's approach, with Dr. Andrew James outlining a comprehensive and institutionalized framework combining research and innovation security.

Across the series, discussions were moderated by ISDP representatives,

including Dr. Niklas Swanström, ISDP Executive Director, and Melita Phachulia, ISDP Executive Assistant.

This report synthesizes insights from these sessions, highlighting common trends, key differences, and emerging policy approaches across countries.

KEY TAKEAWAYS FROM EACH WEBINAR

The Swedish session highlighted that Sweden's highly internationalized research ecosystem represents both a strategic strength and a structural vulnerability. While openness and global collaboration have underpinned Sweden's innovation capacity, they also increase exposure to foreign interference and intellectual property risks. The discussion emphasized that Sweden lacks a comprehensive national framework for research-related intellectual property protection, and that "responsible internationalization" is emerging as the primary guiding principle for balancing openness with security considerations.

It was further stressed that research security is not only a regulatory issue but also a cultural one, requiring institutional awareness and behavioral change. Sweden, while reflecting broader European Union (EU) trends, was discussed as a distinct national case, while the wider European context remains in an adaptive phase of developing more structured approaches.

The U.S. session underscored that nearly all advanced scientific research now carries dual-use potential, which complicates traditional approaches based on controlling specific technologies. The discussion highlighted a clear shift toward actor- and partner-based risk assessment, where geopolitical context and institutional affiliations play a central role.

Public funding was identified as the primary policy tool for enforcing research security, linking compliance to federal support. At the same time, research security was framed as an issue closely connected to economic competitiveness and technological leadership. A recurring concern was the limited capacity of universities to independently manage complex geopolitical risk assessments.

The subsequent session examining the effectiveness of U.S. research security policies highlighted significant implementation gaps. Although policy frameworks exist, many remain advisory and inconsistently enforced, allowing high-risk collaborations to continue, including with PRC defense-linked institutions. The discussion emphasized persistent transparency gaps in funding disclosure and institutional oversight, as well as fragmentation across federal agencies that undermines clear implementation.

A key conclusion was the need for a centralized framework capable of standardizing risk assessment, improving enforcement, and strengthening coordination across agencies.

The Estonian session presented a distinct model focused on cybersecurity and digital resilience. Estonia's approach is built on a whole-of-society framework that integrates government institutions, the private sector, and civil society actors. A central insight was that cybersecurity resilience depends heavily on human behavior, digital literacy, and public awareness. High levels of institutional trust and transparency were identified as foundational to Estonia's digital governance system.

The discussion further highlighted continuous training, simulations, and cross-sector coordination as essential elements of resilience. Cybersecurity was also framed as closely interconnected with hybrid threats, including disinformation and geopolitical conflict.

The UK session emphasized a highly institutionalized and structured approach to research and innovation security. A key analytical distinction was drawn between research security, which focuses on protecting academic knowledge, and innovation security, which addresses risks in commercialization and investment environments.

The UK has developed a comprehensive framework combining regulatory instruments, advisory bodies, and awareness initiatives. The discussion also noted a shift toward a "de-risking" approach, particularly in relation to China, although this has been associated with unintended "chilling effects" on international collaboration. Implementation challenges remain, especially among smaller institutions, where capacity and awareness vary significantly.

DIFFERENCES BETWEEN COUNTRIES AND PRACTICES

Significant variation exists in how countries structure governance and implement research security policies. The UK represents the most institutionalized model, characterized by centralized coordination, dedicated agencies, and structured advisory mechanisms. The U.S., while gradually moving toward stronger coordination, remains fragmented across multiple agencies, with many measures still advisory in nature. Sweden and the broader European context reflect a more decentralized and evolving approach, relying heavily on soft governance tools and the principle of responsible internationalization. Estonia reflects this broader European approach while distinguishing itself through a whole-of-society model, where cybersecurity and resilience are integrated across state institutions, private sectors, and civil society.

Differences are also evident in policy instruments. The U.S. relies heavily on public funding as a lever for shaping compliance, while the UK combines regulatory frameworks with advisory

and awareness-based tools. Sweden and the EU primarily depend on non-binding guidelines and normative approaches, whereas Estonia integrates legal frameworks with strong emphasis on behavioral resilience and digital literacy.

Approaches to risk assessment also diverge. The U.S. and UK apply actor-centered and geopolitically informed risk models, whereas Sweden and the EU are still developing structured frameworks. Estonia, by contrast, focuses less on research partnerships and more on systemic vulnerabilities, particularly human behavior and cyber risks.

Similarly, the scope of research security varies, with the U.S. and UK expanding into economic and innovation security, while Sweden and the EU remain more focused on academic research and intellectual property protection. Estonia adopts the broadest framing, linking cybersecurity, digital governance, and societal resilience.

Finally, approaches to international collaboration differ significantly. The U.S. has adopted a more restrictive and strategic stance, the UK has pursued managed de-risking, Sweden continues to prioritize openness with emerging safeguards, and Estonia maintains openness within a highly secure digital governance environment.

SIMILARITIES ACROSS COUNTRIES AND PRACTICES

Despite differences in institutional design and policy maturity, several common trends are evident across all cases. Research and innovation security is now widely recognized as a strategic policy domain rather than a narrow technical issue. Advanced scientific research is widely understood to have dual-use potential, blurring the boundaries between civilian and military applications. This has contributed to a broader shift toward risk-based governance approaches, where the focus is primarily placed on actors, partnerships, and geopolitical context rather than technologies alone.

Another shared trend is the presence of institutional capacity gaps, particularly within universities and research organizations that often lack the expertise and resources needed to conduct complex risk assessments. At the same time, all cases reflect a persistent tension between maintaining openness in scientific research and addressing growing security concerns. Despite differing policy responses, international collaboration remains a core component of research ecosystems, although it is subject to scrutiny and conditionality.

CONCLUSION

The Research and Innovation Series demonstrates that research and innovation security is emerging as a central dimension of national security and economic policy across advanced democracies. While all countries are responding to similar structural pressures, including dual-use technologies, geopolitical competition, and foreign interference risks, their policy responses diverge significantly based on institutional capacity, governance traditions, and strategic priorities.

A clear global trend toward the securitization of research and innovation is evident. However, this trend is being interpreted and operationalized in different ways, ranging from centralized and security-driven systems to openness-oriented and resilience-based models. The key policy challenge lies in balancing the protection of strategic interests with the preservation of scientific openness and international collaboration.

Addressing this challenge will require stronger institutional capacity, improved coordination mechanisms, and more coherent risk assessment frameworks. It will also require sustained investment in trust, transparency, and societal resilience. Ultimately, the effectiveness of research and innovation security policies will depend on the ability of states to develop adaptive governance models capable of responding to rapidly evolving technological and geopolitical conditions without undermining the foundations of scientific progress.

WATCH ON YOUTUBE

Part I: Swedish Perspectives on Research and Innovation Security	SEP 9, 2025
Part II: US Perspectives on Research and Innovation Security	JAN 28, 2026
Part III: Are US Research Security Policies Working?	FEB 27, 2026
Part IV: Cybersecurity and Digital Resilience: What Europe can Learn from Estonia	MAR 17, 2026
Part V: UK Perspectives on Research and Innovation Security	MAR 31, 2026

Institute for Security and Development Policy
Västra Finnbodavägen 2, 131 30 Nacka, Sweden
www.isdp.eu | info@isdp.eu