SAND2025-03951R

Enhancing Research Security in Latvia and Estonia: Potentials for Mitigating China-related Risks in Academic Collaboration

Dr. Solvita Denisa-Liepniece

Dmitri Teperik

March 2025

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

ABSTRACT

Having studied various vulnerable groups and communities in the Baltics and beyond for decades, the report's authors have come to understand that academia is being targeted and misused by foreign autocratic regimes (i.e. Russia, China, etc.) for various malicious purposes: from espionage to influence operations.

This study report aims to present the current state of affairs and to guide stakeholders in Latvia and Estonia in emphasizing the importance of a broader security culture in academia and research. It is conceivable that the topic could be actualized for both communities of practitioners – security and academia – by bridging issues of personal safety, reputational risks as well as institutional, national and regional security.

As the report deals with complex issues and relations between different cultures, the authors acknowledge the importance of academic freedom and functional autonomy of universities and research institutions. Therefore, this report could serve as a pioneering reference for Latvian and Estonian stakeholders in the field of research security.

ACKNOWLEDGEMENTS

The authors would like to express their sincerest gratitude to the U.S. State Department, the U.S. Department of Energy, and Sandia National Laboratories for their invaluable support in enabling the Visiting Research Scholar Program, which has resulted in this publication.

The authors would like to extend their gratitude to Mr. Chris Cutrone of Sandia National Laboratories, who was very helpful and instrumental in establishing this fruitful fellowship and facilitated collaborative engagement in an exemplary manner.

The authors would like to thank the interviewees from Latvian and Estonian organizations, whose views, comments, and remarks helped constructively in the course of the study and later in the preparation of the report.

The authors believe that Baltic academic communities can benefit from a security mindset, as it helps to safeguard and protect values across borders, sectors, and domains.

CONTENTS

EXECUTIVE SUMMARY

Russia's unprovoked aggression against Ukraine has a significant impact on perceptions regarding the moral and legal implications of international research collaboration with authoritarian regimes. In contrast to the situation with Russia (and Belarus), navigating the complexities of Chinese influence in academia is more challenging, particularly in the absence of clear guidelines or principles on research security.

Western research policy decision-makers are confronted with the challenge of determining the optimal balance between the imperative of intensifying collaboration with China, which is experiencing a rapid expansion in the number of scientific and technological articles and patents, and the security concerns associated with espionage, the misuse of intellectual property rights, and the potential for dual-use applications.

Security concerns pertaining to China's scientific and technological advancements are related to the concept of cognitive warfare, which is further reinforced by its integration with "intelligentized" warfare to utilize various emerging technologies and artificial intelligence. When viewed through the lens of irregular warfare strategy, China's global competition strategy encompasses both traditional and non-traditional espionage, as well as influence activities targeting Western universities, research entities, non-governmental organizations, and public institutions.

The potential risks associated with interactions with China have been examined in Latvia and Estonia through the lens of national security. The authorities have primarily focused on enhancing the protection of government agencies and their officials, as well as raising awareness about the vulnerabilities of 5G and other technologies that may be directly or covertly controlled by China. Some researchers have noted that the manifestations of Chinese influence activities in Latvia and Estonia are comparable, yet each country exhibits distinctive characteristics.

The objective of this research study is to identify the key elements that could potentially be exploited by China in its influence activities within the major Latvian and Estonian universities, as well as their staff and students. Consequently, the study focuses on a number of vulnerabilities with the aim of assessing the general level of preparedness of key Latvian and Estonian academic organizations for addressing China-related threats and providing recommendations on the instrumentalization of operational security within Latvian and Estonian academia. The majority of local universities are still in the initial stages of developing the capacity to identify plausible foreign-origin threats to research security and to mitigate the risks within established legal frameworks, as well as within the context of its long-standing traditions of academic freedom and resource constraints.

In light of the aforementioned risk analysis and the subsequent application of best practices in risk mitigation, the recommendations for Latvia and Estonia are based on the 4Cs approach (4C – Commitment, Collaboration, Communication, and Control). It is recommended that Latvia and Estonia continue to engage in discourse and the formulation of policies at the personal, institutional, and potentially national levels with the aim of mitigating security risks within the academic domain and promoting the implementation of research integrity practices. In order to guarantee the safeguarding of critical research assets, it would be advisable to assess and evaluate the potential risks associated with collaborative engagement with non-democratic regimes and implement suitable preventive measures in accordance with the guidance provided by security authorities. The establishment of the Baltic Research Security Network of Practitioners would be beneficial for the coordination, collaboration, and exchange of best practices for the rapid dissemination of information on due diligence issues and risk mitigation between the academic communities of the Baltic region.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ASCE	Academic Security and Counter Exploitation Program
ASPI	Australian Strategic Policy Institute
BGI	Beijing Genomics Institute
CCP	Chinese Communist Party
CEE	Central and Eastern Europe
COE	centre of excellence
C4	commitment, collaboration, communication, and control
C4I	command, control, communications, computers, and intelligence
DOD	United States Department of Defense
DOJ	United States Department of Justice
EU	European Union
FBI	Federal Bureau of Investigations
HEI	higher education institution
IPR	intellectual property rights
KAPO	*Kaitsepolitseiamet* (Estonian Internal Security Service)
LSM	*Latvijas sabiedriskais medijs* (Latvian Public Media)
NATO	North Atlantic Treaty Organisation
NCSC	National Counterintelligence and Security Center
NIH	National Institutes of Health
NIST	National Institute of Standards of Technology
NGO	non-governmental organisation
NSF	National Science Foundation
PLA	People's Liberation Army
PRC	People's Republic of China
R&I	research and innovation
SAB	*Satversmes aizsardzības birojs* (Latvia's Constitution Protection Bureau)
S&T	science and technology
UK	United Kingdom
US	United States

1. INTRODUCTION

The global geopolitical landscape is witnessing an intensification of hybrid threats, which are challenging and endangering open societies through the actions of both state and non-state actors. International academic cooperation can become a potential national security risk, as the rules and norms that apply in the EU or the US should not be expected to be followed by the non-democratic regimes. Consequently, there is a need to endorse security strategies and programs within academia to protect against rising threats.

Latvia and Estonia have been countering various threats posed by Russia's malign influence campaigns over the last decades. As the efficiency of the countermeasures vary widely across different areas, the current situation remains complex and suggests that there are some security gaps in attitudes on, awareness about and preparedness for mitigating the risks when it comes to cognitive warfare executed by actors other than Russia. Although the influence activities of the People's Republic of China (PRC) don't yet demonstrate a high level of overt hostility as in Russia's case, China's intentions regarding the West in general have the nature of growing confrontation or even adversity. A GLOBSEC study has revealed a notable increase in the proportion of the population in Latvia and Estonia who perceive China as a security threat to their country. This trend can be observed when comparing the data from 2022 and 2024.[1] In addition to shaping the China-related perceptions of political and intellectual elites in Latvia and Estonia, Chinese intelligence has specific interests in certain areas such as technologies, infrastructure, and industry. It places scientific establishments and higher education institutions (HEI) on the priority target list of China's influence and possibly also espionage activities.[2]

"A Guide to Responsible Research" describes the major risks that impact science and research misconduct, paying more attention to the issues of safety, integrity, and ethics, but not security.[3] Certain vulnerabilities arise when higher education and research stakeholders are unaware that international cooperation and science can be politicized or weaponized, which leads to the abuse of the concept of academic freedom. Since cognitive warfare operates in the human domain across different organizations, it can naturally target the most vulnerable - those who lack proper understanding and regular practice of operational security. Therefore, if unprepared, academia in general, and in Latvia and Estonia in particular, might remain susceptible to malicious attacks or manipulation.

The intricate matter of research security and its interconnectivity with research integrity has been addressed in the JASON report of 2023 on the "Research Program on Research Security." The document posits that the research program on research security would be beneficial in addressing numerous concerns pertaining to foreign influence and the security of the U.S. fundamental research ecosystem. A multitude of topics could be the subject of such a research program, and the majority

[1] GLOBSEC. (2024). *GLOBSEC Trends 2024*. Retrieved on December 16, 2024 from www.globsec.org/sites/default/files/2024-05/GLOBSEC%20Trends%202024.pdf.
[2] Putter, Dries, and Sascha-Dominik Bachmann. "Russia and China Expected to Renew Their Espionage Vigour." *Journal on Baltic Security*, vol. 9, no. 1, 2023, pp. 1-31. https://doi.org/10.57767/jobs_2023_0002.
[3] *Research Security: Safeguarding U.S. Research in a Changing Global Context*. Springer, 2024. Retrieved on December 16, 2024 from https://link.springer.com/book/10.1007/978-3-031-22412-6

of these would benefit from close collaboration with social scientists and the integration of their insights with those of practicing natural scientists in the relevant fields.[4]

Security concerns about China's scientific and technological advancements are related to the concept of cognitive warfare, which is further reinforced by its integration with "intelligentized" warfare–China's new military strategy–which focuses on using artificial intelligence and is characterized by four key features: increased information-processing capabilities, rapid decision-making, the use of swarms, and cognitive warfare.[5] Moreover, China's ambitions are reflected in the decision of the People's Liberation Army (PLA) to establish, among other new forces, the Information Support Force with the objective of strengthening its psychological warfare capabilities.[6] When viewed through the lens of irregular warfare strategy, China's global competition strategy encompasses both traditional and non-traditional espionage, as well as influence activities targeting Western universities, NGOs, and public organizations, as China has the objective of influencing future decision-making processes in the West and enhancing China's competitive advantages in technological and cognitive domains.[7]

Another indication of the weaponization of information and cognitive domains in China is the establishment of the Committee on the Cultural Metaverse by the China Cultural Industry Association in 2022. This is described as China's industry–university collaborative innovation to enhance domestic and international exchange and cooperation in the cultural domain. The enterprise engaged more than 120 scholars from more than 20 Chinese universities and has been described as a comprehensive, systematic, and in-depth analysis and interpretation of the fundamental theory and industrial practice of cultural metaverse in China. The whole work has been coordinated by the Propaganda Department of the Chinese Communist Party's Central Committee and contributed to the Chinese propaganda system, the activities of which resulted in the exploitation or use of new and emerging technologies.[8] Moreover, China views science and technology as a central instrument for advancing its strategic and geopolitical objectives in the international arena. This perspective is reflected in the Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 as follows: "We will intensify the opening up of the national S&T programs, launch a number of major S&T cooperation projects, look into the establishment of a global scientific research fund, and implement a scientist exchange program. We will support the establishment of international S&T organizations within China, and foreign scientists filling positions in Chinese academic S&T organizations"[9].

In pursuit of its goal of having a fully modernized military by 2035 and a globally competitive military by 2049, the Chinese PLA engages in extensive collaboration with military and civilian companies in the information and technology sectors, particularly in the context of C4I (Command, Control,

---

[4] National Science Foundation. (2023). *NSF Research Program on Research Security*. Retrieved on December 16, 2024 from https://nsf-gov-resources.nsf.gov/2023-03/JSR-22-08%20NSF%20Research%20Program%20on%20Research%20Security_03152023_FINAL_1.pdf.

[5] Schlesinger, Robert. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." *War on the Rocks*, July 2022. Retrieved on December 16, 2024 from https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine.

[6] Payne, Christopher. "Farewell to China's Strategic Support Force: Let's Meet Its Replacement." *Defense One*, April 2024. Retrieved on December 16, 2024 from www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143.

[7] *The Future Faces of Irregular Warfare*. Irregular Warfare Center. Retrieved on December 16, 2024 from https://irregularwarfarecenter.org/publications/the-future-faces-of-irregular-warfare.

[8] Australian Strategic Policy Institute. *Truth and Reality: Chinese Characteristics*. Retrieved on December 16, 2024 from www.aspi.org.au/report/truth-and-reality-chinese-characteristics.

[9] Georgetown University Center for Security and Emerging Technologies. *14th Five-Year Plan* [PDF]. Retrieved on December 16, 2024 from https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

Communications, Computers, and Intelligence) operations. Companies and research establishments that develop dual-use technologies are involved in the core operations of the PLA Information Support Forces and the development of an integrated Military Network System across different domains, including information acquisition, information transmission, information processing, information security, military electronic components, and military simulation.[10]

A challenge for Western research policy decision-makers is to determine the optimal balance between the imperative of intensifying collaboration with China, which is experiencing a rapid expansion in the number of scientific and technological articles and patents, and the security concerns associated with espionage, the misuse of intellectual property rights (IPRs), and the potential for dual-use applications.[11] However, as noted in the report of the annual US-China Strategic Dialogue 2024, U.S. and Chinese participants were optimistic that the two countries can preserve economic and scientific cooperation that is mutually beneficial, keeping national security restrictions to a minimum.[12]

To meet the growing challenges of cognitive warfare, the U.S. has identified key areas for investment, including communications, human capital, information access and cognition, and proactive influence and predictive analytics. These efforts will enable the advancement of cognitive operations across government and society, including media, academia, and NGOs.[13] At the same time, while the demand for research security increases exponentially, there are only a limited number of available tools for universities and research entities that lack the requisite expertise to assess the inherent risks associated with academic collaboration with China.[14]

As recommended in the multinational study "Mitigating and Responding to Cognitive Warfare" published by the NATO Science and Technology Organization, cross-sectoral implementation of cognitive security is required to defend information security and reliability that is essential for maintaining trust and decision-making within the Alliance. This includes shared situational awareness and sensemaking as well as a collaborative approach for 'plugging into' technology development. This is to leverage industry and academic investments in state-of-the-art technologies and analysis methods to ensure optimal performance enhancement and information transfer.[15]

This research study aims at identifying key elements that could be exploited by China in influence activities within the major Latvian and Estonian universities, as well as their staff and students. For that reason, the study focuses on several vulnerabilities to assess the general level of preparedness of key Latvian and Estonian academic organizations for addressing the China-related threats and to provide recommendations on instrumentalizing operational security within Latvian and Estonian academia.

---

[10] USANAS Foundation. "Decoding the Role of Chinese Military Companies Operating with the PLA Information Support Force (ISF): A Comprehensive Analysis." Retrieved on December 16, 2024 from https://usanasfoundation.com/decoding-the-role-of-chinese-military-companies-operating-with-the-pla-information-support-force-isf-a-comprehensive-analysis-of-the-major-military-companies.

[11] "How Worrying Is the Rapid Rise of Chinese Science?" *The Economist*, June 13, 2024. Retrieved on December 16, 2024 from www.economist.com/leaders/2024/06/13/how-worrying-is-the-rapid-rise-of-chinese-science.

[12] National Center for Academic Freedom and Privacy. *U.S.-China Research Security Report 2024*. Retrieved on December 16, 2024 from https://ncafp.org/wp-content/uploads/2024/07/FINAL-U.S.-China-Report-2024.pdf.

[13] Haugland, Edward Lawrence. *The Cognitive War: Why We Are Losing and How We Can Win*. 2023.

[14] Science Business. *The Future of Research Security*. Retrieved on December 16, 2024 from https://sciencebusiness.net/node/59046/preview/LChyxFBPZ4bPPCkf_wYS1K_Aif0RkRXpnHL9HU747K8.

[15] NATO Science and Technology Organization. *STO-TR-HFM-ET-356: Research Security and Technology Innovation*. Retrieved on December 16, 2024 from www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$$TR-HFM-ET-356-ALL.pdf.

2. LITERATURE REVIEW

This literature review commences with a differentiation between threat framework and risk mitigation in the United States, before progressing to threat perception in Estonia and Latvia-focused research. Furthermore, several European references are provided in brief to illustrate the complexity of the issue. While establishing the context with the recent literature addressing the issue of foreign influence and countering foreign influence in academia, the overview is limited to international collaborations, reflecting the prioritization of the issue in the available sources on national security and academia. In particular, this study presents a comprehensive overview of the various mechanisms that have been identified as being employed by non-democratic regimes. This provides the foundation for a subsequent analysis of the available countermeasures.

The available research studies on Chinese influence in the Baltics address mainly strategic threats from geopolitical, technological, and economic points of view. In contrast, challenges to knowledge/research security within academia are analyzed on a limited number of cases. This may indicate that Latvian and Estonian universities and research institutions are still in the early stages of learning how to identify plausible foreign-origin threats to their operational security and how to mitigate the risks within established legal frameworks, as well as within the context of their long-standing traditions of academic freedom and financial challenges.

The methodology employed in the study may be characterized as descriptive. Nevertheless, the authors do not focus on any specific individual case of influence, but rather make reference to the more or less used mechanisms. As G. Tiffert, a specialist on the Chinese legal system, wrote, "It would be a grave error to mistake the comparatively low number of publicized cases that dramatize these challenges as evidence that existing safeguards are sufficient or as grounds for complacency."[16] In this study, the authors deliberately refrained from focusing on specific instances of influence[17] identified in academic literature. Instead, a number of initiatives designed to enhance awareness and mitigate risk is presented.

[16] Tiffert, Glenn. *Global Engagement: Rethinking Risk in the Research Enterprise*. Hoover Institution Press, 2020.
[17] U.S. Department of Energy. "Countering Foreign Interference in Department-Funded Research Institutions of Higher Education." *NIH Foreign Interference Report*, 2023. Retrieved on December 16, 2024 from https://grants.nih.gov/sites/default/files/Foreign-Interference-8.22.pdf.

2.1. 2.1 U.S. national security risks in academia and scientific cooperation

The first part of this literature overview section on national security risks in academic and scientific cooperation is focused on U.S. examples to provide a better understanding of methods used by the Chinese government. The second part of this section addresses methods of effective response with a set of techniques (the best practices). Both, as mechanisms of influence and countermeasures, are interconnected, constantly being updated and are equally important to limit unwanted foreign influence in HEIs and research establishments. The first part not only proves the relevance of the whole-of-society approach to national security and academia, but also raises a need for developing security programs within universities and research institutions.

2.1.1. Risks

The United States National Counterintelligence Strategy of 2024 identifies the protection and defense of critical technologies, sensitive data, and the national innovation base as a matter of the utmost importance.[18] While academic collaborations provide significant benefits, when it come to a collaboration with non-democratic regimes, including China and Russia, benefits could entail serious risks. The development of technology and science superpower is used by China in the advancement of its military power.[19] Military–civil fusion creates significant risks. The most recent annual threat assessment of the U.S. Intelligence community pays attention to four state actors: China, Russia, Iran, and North Korea. Regarding China, the report said, "The PRC combines its economic heft with its growing military power and its diplomatic and technological dominance for a coordinated approach to strengthen Chinese Communist Party (CCP) rule, secure what it views as its sovereign territory and regional pre-eminence, and pursue global power."[20] Non-democratic regimes try different ways to participate in Western collaborative academic environments. While contributing to academic and research success, the openness of academic institutions may also be used by these regimes to pursue their agenda. Sponsored economic espionage is not the only characteristic of non-democratic regimes.

As stated in the JASON report of 2019 on Fundamental Research Security, actions of the Chinese government and its institutions that are not in accord with U.S. values of science ethics have prompted concerns about foreign influence in the U.S. academic sector. The report provides an excellent background on the history and current state of foreign influence in U.S. fundamental research, as well as highlighting the need to extend our notion of research integrity to include disclosures of commitments and potential conflicts of interest. Furthermore, the report calls for a shared understanding between academia and U.S. government agencies on the optimal means of safeguarding U.S. interests in fundamental research while maintaining an open environment and successfully competing in the global marketplace for scientific talent.[21]

According to the Federal Bureau of Investigations (FBI), Chinese development strategy includes "every opportunity – from academic collaborations to economic espionage – to develop and maintain

[18] National Counterintelligence and Security Center. *NCSC CI Strategy*. July 30, 2024. Retrieved on December 16, 2024 from www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf.
[19] Laskai, Lorand. "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise." *Council on Foreign Relations*, 2018. Retrieved on December 16, 2024 from www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise.
[20] Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. February 2024.
[21] National Science Foundation. *Fundamental Research Security*. December 6, 2019. Retrieved on December 16, 2024 from www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

a strategic economic edge."[22] To achieve economic, technological, and military goals, the FBI's report highlighted that China's government has 100 plans "guiding China's foreign acquisitions", including the 14th Five-Year Plan and The Made in China 2025 Plan. Industries mentioned in "The Made in China 2025 Plan" include: Informational technology; Computer numerical control machine tools and robotics; Aerospace equipment; Marine engineering equipment and high-tech ships; Advances rail transportation equipment; Energy-efficient and new energy automobiles; Electric power equipment; Agricultural equipment; New materials; Biomedicine and high-performance medical instruments. One of the ambitions of the PRC's "Made in China 2025" initiative is to become a dominant force in high-tech manufacturing to achieve self-sufficiency in core technologies such as semiconductors, robotics and artificial intelligence. This goal will have geopolitical and security implications for the West, as there are concerns about intellectual espionage and tensions over Chinese technologies being used for strategic advantage.[23]

For those working in these environments, the FBI report emphasized, "expect foreign adversaries to target it." FBI warns that even information that could seem insignificant may be targeted, as "by bypassing the research and development phase and stealing your technological information or product, foreign adversaries can gain a competitive economic and military advantage."[24] Same goes to the currently unclassified, but potentially national security relevant applications.

The FBI notes the following potential targets within academia: students, professors, and researchers with access to research and technical information (particularly graduate and postdoctoral students). There is a great variety of data and documentation which espionage actors may be interested in: pre-publication research results; research data; techniques and processes; laboratory equipment and software; pre-classification research; access protocols; budget estimates and expenditures; computer access protocols; computer network design; customer and employee data; equipment specifications; passwords for your computer, phone, or accounts; phone and property data; proprietary research, formulas, and processes; prototypes or blueprints; software, including source codes; technical components and plans; vendor information and supply chain; grant data.

Among the tactics mentioned are "joint research opportunities, language and cultural training, unsolicited invitations, visiting students and professors, and state-sponsored industrial and technical espionage to support their military and commercial research, development, and acquisition."[25] The following issues are listed: talent recruitment or "brain gain" programs; foreign students or visiting professors; language and cultural training; funding and donations; elicitation; joint research opportunities; foreign travel; foreign visitors.

While the FBI bulletin is focused on critical technologies, the relevance of social sciences with a focus on cognitive sciences should not be overlooked. The Japanese National Institute for Defense Studies noted in the recently published report entitled "China's Quest for Control of the Cognitive Domain and Gray Zone Situations": "In future wars, the information domain will certainly play a more

---

[22] FBI. *China: The Risk to Academia*. 2019. Retrieved on December 16, 2024 from www.fbi.gov/file-repository/china-risk-to-academia-2019.pdf/view.

[23] Center for Strategic and International Studies. "Made in China 2025." *CSIS Analysis*. Retrieved on December 16, 2024 from www.csis.org/analysis/made-china-2025.

[24] FBI. *China: The Risk to Academia*. 2019. Retrieved on December 16, 2024 from www.fbi.gov/file-repository/china-risk-to-academia-2019.pdf/view.

25 *Ibid.*

important role, will further elevate its status, and gradually play a leading role that supersedes firepower."[26]

The importance of social sciences was also highlighted in China's "Outline of the 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035" as follows, "We will construct curricula systems, academic systems, and discourse systems for philosophy and social sciences with Chinese characteristics, implement philosophy and social science innovation projects in an in-depth manner, and strengthen the construction of new think tanks with Chinese characteristics."[27]

The Global Engagement Center's Special Report on "How the People's Republic of China Seeks to Reshape the Global Information Environment" highlights that the information available to the public, media, civil society, academia, and governments in engaging with China could be distorted by propaganda and disinformation and limited by censorship. This would pose a direct challenge to all nations that seek to base their relations with China on fact-based assessments of their sovereign interests.[28]

P. Charon and J.-B. Jangle Vilmer authored the book *Chinese Influence Operations. A Machiavellian Moment*, which analyzed the main actors and actions employed abroad by the Chinese government. Along with the use of diaspora, the media, diplomacy, policy, economy, think-tanks, culture, and information manipulations, they also provided detailed analysis of influence operations through education. The authors echoed the FBI's list, providing examples from the across the world on financial dependence, elite capture, pressure by Chinese students, pressure on publishers, PhD supervisors, or relatives in China; arrests and intimidations for those with access to their field in China, kidnapping, arbitrary arrests, disappearance, force televised "confessions" of activists, journalists, publishers, and critics of Beijing, and self-censorship.[29] Moreover, as evidenced by the case of Finnish universities, Chinese students are engaged in the practice of ideological espionage towards one another, as well as in the conduct of possible espionage activities within research organizations.[30]

As mentioned above, Charon and Jangle Vilmer separately looked at the utilization of think-tanks in the context of influence operations. According to the authors, think-tanks are used to reinforce Chinese presence in the international debate. Both Chinese think-tanks and attempts to engage with non-Chinese think-tanks are named. Moreover, the authors wrote "China specifically targets Central and Eastern European countries."[31] Three types of Chinese influence are mentioned: occasional partners, circumstantial allies, and accomplices.

Since the CCP is building connections between environments inside the country, the whole-of-government approach combines the civilian sector, including universities, with the military and

---

[26] Shinji, Y., et al. (2023). "China's Quest for Control of the Cognitive Domain and Gray Zone Situations." *National Institute for Defence Studies*.
[27] Georgetown University Center for Security and Emerging Technologies. *14th Five-Year Plan* [PDF]. Retrieved on December 16, 2024 from https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.
[28] U.S. State Department. *GEC Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment*. Retrieved on December 16, 2024 from www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment.
[29] Charon, P., and Jeangène Vilmer, J.-B. *Chinese Influence Operations: A Machiavellian Moment*. Institute for Strategic Research, 2021.
[30] Yle. "Chinese Military Strategy: What Are the Plans for the Next Decade?" *Yle News*, 2024. Retrieved on December 16, 2024 from https://yle.fi/news/2024/01/19/chinese-military-strategy-plans-next-decade.
[31] Charon, P., and Jeangène Vilmer, J.-B. *Chinese Influence Operations: A Machiavellian Moment*. Institute for Strategic Research, 2021.

security sectors.[32] According to the report, 15 civilian universities in China were active in 2019. The Australian Strategic Policy Institute provides a list of universities with very high, high, medium and low risks based on ties to the Chinese military and defense industry. For instance, several reports, including "Global Engagement: Rethinking Risk in the Research Enterprise," flag the Seven Sons of National Defense as an example of "risky" institutions. Also, the state-owned defense industry tries to increase its overseas presence.

For example, the China Defense Universities Tracker names the following 12 defense industry conglomerates: China South Industries Group; China Electronics corporation; China Electronics, Technology Group Corporation; China National Nuclear Corporation; China Aerospace Science and technology Corporation; Aviation Industry Corporation of China; Aero Engine Corporation of China; Commercial Aircraft Corporation of China; China Shipbuilding Industry Corporation; China State Shipbuilding Corporation; China North Industries Group - Norinco Group.[33]

In the summary of Foreign Interference Cases detected in National Institutes of Health (NIH), M. Lauer wrote that few cases led to criminal cases and while "the most common source was internal, that is agency staff discovering discrepancies in grant documents and published materials."[34] The importance of raising awareness and some risk mitigation practices are collected in the next section of the analysis.

2.1.2. Risk Mitigation

While the previous section answered the question "How the influence activities can be performed?", the current one is focused on another type of "how" – how to build the know-how to mitigate risks. Within the last few years, thanks to increased visibility of previously hidden activities, different stakeholders developed knowledge-sharing strategies and tools and started to disseminate best practices in combating emerging threats. Within the last few decades, risk mitigation evolved from single initiatives towards a whole-of-society approach in some Western countries, including the U.S. This section focuses on describing U.S. mitigation practices due to their advanced understanding of the threat and sharpened risk perceptions. However, to apply these findings to the Latvian and Estonian contexts, further analysis and adaptation to the EU legislative environment would be necessary.

A ground-breaking initiative, the "Academic Security and Counter Exploitation Program (ASCE)" started in 2006 at the Texas A&M University System. Almost ten years later, in 2015, the first Academic Security and Counter Exploitation Training Seminar was established. Opening the seminar in 2021, K.R. Gamache said, "The conference has grown since that first year to include the broader academic community and increased federal engagement from the FBI, DOJ, DOD, NSF, NIH, Office

[32] Joske, A. "Front Matter." *The China Defence Universities Tracker: Exploring the Military and Security Links of China's Universities*. Australian Strategic Policy Institute, 2019. http://www.jstor.org/stable/resrep23061.1.
[33] Ibid.
[34] U.S. Department of Energy. "Countering Foreign Interference in Department-Funded Research Institutions of Higher Education." *NIH Foreign Interference Report*, 2023. Retrieved on December 16, 2024 from https://grants.nih.gov/sites/default/files/Foreign-Interference-8.22.pdf.

of the Director of National Intelligence, and Office of Science and Technology Policy."[35] Taking the leading role, the program provides a set of resources and serves as a network.

The U.S. government integrates research security into national and institutional frameworks for research integrity. For instance, the Memorandum for Under Secretary of Defense for Acquisition and Sustainment (Secretary of the Army; Secretary of the Air Force; Secretary of the Navy; Commander, United States Special operations Command; Commander, United States Cyber Command; Commander United States Strategic Command; Director, Missile Defense Agency; Director, Defense and Advanced Research Projects Agency; Director, Defense Threat Reduction Agency), signed in June 2023, stated that "Many in the academic community were unaware of the research security risks associated with some foreign governments, including through foreign government-sponsored talent recruitment programs, before the Department and other Federal agencies began taking action to inform academia of these threats."[36]

The document provides a comprehensive list of mitigation strategies. For instance:

- Require the covered individuals to complete insider risk awareness training;
- Require increased frequency of reporting by the covered individuals(s);
- Replace individuals listed in the fundamental research project proposal who are deemed a research security risk;
- Provide DoD the covered individual's (s') contracts for review and clarify relationship, affiliations, and / or associations considered risky;
- Require the covered individuals(s) to resign from positions deemed problematic by the risk based security review.

The document provides not only a list of universities, but also points out Foreign Talent Programs "that pose a threat to National Security Interests of the United States," including but not limited to: Changjiang Scholar Distinguished Professorship; Hundred Talents Plan; Pearl River Talent Program; Project 5-100; River Talents Plan; Thousand Talents Plan.

Legislation, guidelines, tools and even templates and quizzes, among other activities, are aimed to protect national security by bringing awareness to the agenda.[37] Research security in the U.S. is also promoted on the political level, e.g. within the National Science and Technology Council's subcommittee on research security[38]. There is a growing number of these types of activities, with several turning points,[39] including a DoD letter to the academic community regarding the risk of

---

[35] Gamage, K. 2022. *Statement for the Record: Nomination of Avril Haines to be Director of National Intelligence.* U.S. Senate Select Committee on Intelligence. Retrieved on December 16, 2024 from www.intelligence.senate.gov/sites/default/files/os-kgamache-092122.pdf.

[36] Department of Defense. 2023. *Countering Unwanted Influence in Department-Funded Research at Institutions of Higher Education.* Retrieved on December 16, 2024 from https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

[37] American Institute of Physics. 2023. "DoD to Screen Researchers for Risky Foreign Ties." *FYI - The AIP Bulletin of Science Policy News.* Retrieved on December 16, 2024 from https://ww2.aip.org/fyi/dod-to-screen-researchers-for-risky-foreign-ties.

[38] The White House. 2022. *NSPM-33 Implementation Guidance.* Retrieved on December 16, 2024 from www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

[39] U.S. Congress. 2022. Public Law 117-167: CHIPS and Science Act of 2022. Retrieved on December 16, 2024 from www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf.

improper foreign interference.[40] Symbolically, one of several links in the letter leads to the ASCE initiative. Also, DoD developed a matrix of risk factors.[41] The matrix includes the following four factors: Foreign Talent Recruitment Programs; Funding Sources; Patents; and Entity Lists. In order to show transformation of the legislation, the matrix shows an evolution of measures for cases with 1) prohibited factors; 2) factors discouraged by DoD, mitigation measures requirements, rejection of no mitigation possible; 3) mitigation measures recommended; 4) mitigation measures suggested and 5) no mitigation needed. Analysis of the questionnaire shows close collaboration with threats and risks mentioned in the previous section. The matrix also helps to identify sources for the analysis, as suggested in the document. For instance, analysis of resumes and publications.

There is proof that within the last few years, single initiatives transformed into a holistic approach, engaging with different types of governmental bodies, foundations, and associations. To mention some recent developments, in February 2024, the Committee on Armed Services received testimony on the Department of Defense's programs and initiatives to accelerate innovative technologies, solutions, and capabilities from the research and development enterprise to the war fighter. Talking to the Committee, H. Shyu, Under Secretary of Defense for Research and Engineering, described the intensity of U.S. academic collaborations for outpacing China.[42] Commenting on risks related to engagements with Chinese nationals in U.S. academia, she noted that in 2023, DoD established a policy that focused on academics as well as small businesses. "The policy we have instituted literally requires every grant you are going to receive from us, you have to submit a disclosure. So, in the disclosure you have to talk about affiliation you have, what organization you belong to, what funding are you receiving."

The mentioned disclosure contains eight questions. Definitions like "foreign country of concern" are used in the questionnaire.[43] The document provides the following clarification for "*Foreign country of concern* — As defined in 15 U.S.C. § 638(e)(17), foreign country of concern means the People's Republic of China, the Democratic People's Republic of Korea, the Russian Federation, the Islamic Republic of Iran, or any other country determined to be a country of concern by the Secretary of State."

Another example of collaboration is the "Safeguarding Science Research Security Framework" published in August 2023 by the National Institute of Standards of Technology (NIST). The Framework also provides guidance to assist the U.S. science and research community in securing national interests while focused on international science. The Research Security Framework names the following categories for review: research associate appointments; foreign travel requests; foreign collaborations; foreign requests for products, services, and software tools; extramural funding

---

[40] Stanford University. 2023. "DoD Letter to the Academic Community Regarding Risk of Improper Foreign Interference." *DoResearch*. Retrieved on December 16, 2024 from https://doresearch.stanford.edu/resources/topics/dod-letter-to-acadamic-community-regarding-risk-improper-foreign-interference.

[41] Council on Governmental Relations (COGR). 2022. *Overview of Department of Defense Statement on Countering Unwanted Foreign Influence in Department of Defense-Funded Research*. July 8. Retrieved on December 16, 2024 from www.cogr.edu/sites/default/files/Overview%20of%20Department%20of%20Defense%20Statement%20on%20Countering%20Unwanted%20Foreign%20Influence%20in%20Department%20July%208%2020223.pdf.

[42] House Armed Services Committee. 2023. "Outpacing China: Expediting the Fielding of Innovation." *House of Representatives Hearing*, 2:56:56. Retrieved on December 16, 2024 from https://armedservices.house.gov/hearings/outpacing-china-expediting-fielding-innovation.

[43] Department of Defense. 2024. Disclosures of Foreign Affiliations or Relationships to Foreign Countries. *DoD SBIR/STTR BAA Attachment 2: DFARFC*. Retrieved on December 16, 2024 from https://media.defense.gov/2024/Jan/05/2003369046/-1/-1/0/DoD_SBIR_STTR_BAA_Attachment%202_DFARFC.PDF.

opportunities (for example contracts, grants). The Framework also mentions three main pillars to securing research security - information collection; research security overview; monitoring.[44] Also, the framework suggests the implementation matrix for the safeguarding science research security framework.

Another initiative, led by the National Counterintelligence and Security Center (NCSC), is called "Safeguarding Science".[45] This Outreach Initiative for Protecting Research and Innovation in Emerging Technologies, for instance, promotes collaboration, training, raising awareness, and fostering information exchange. Among their toolkits are a rich collection from specific resources to ready-to-use templates. Considering applicability, the Center provides ready-to-adapt resources, including posters. Thus, in the section "counterintelligence," the most common foreign collection methods are mentioned - request for information; targeting at conferences, conventions and trade shows; foreign visits; academic solicitation; solicitation and marketing/seeking employment; elicitation and requirement; suspicious network activities.[46] Furthermore, this initiative is using gamification in order to help to increase awareness.[47] Sections included in the game include - reporting requirements; foreign travel; cyber counterintelligence; recruiting methodology of foreign intelligence entity; critical infrastructure protection.

The United States National Science Foundation (NSF) has implemented a comprehensive set of measures to ensure the highest standards of research security. The organization employs a Chief of Research Security Strategy and Policy whose office is responsible for equipping researchers with the information and tools related to research security, clarifying security issues and mitigating risks, as well as fostering transparency, disclosure, and other practices that reflect the values of research integrity. NSF measures include various disclosures regarding collaborators and affiliations, biographical sketches, current and pending supports, and conflicts of commitment. Moreover, the NSF runs training and education activities in research security best practices and supports research studies on research security programs. The NSF also has a policy on how to address research security violations with administrative actions such as award suspensions, award terminations, government-wide suspensions of researchers and entities, and/or government-wide debarments.[48]

The U.S. NSF "Guidelines for Research Security Analytics" offer valuable insights into the operationalization of various tools and techniques, including advanced monitoring, conflict of commitment and conflict(s) of interest, digital persistent identifier, human oversight, investigation of potential inconsistency, routine assessment, and verification of inconsistency. The document also enumerates prohibited practices for research security analytics and delineates processes for notification and communication with institutions, as well as procedures for monitoring and reporting.

---

[44] Strouse, G. F. 2023. *Safeguarding International Science Research Security Framework*. NIST Internal Report 8484. National Institute of Standards and Technology. Retrieved on December 16, 2024 from www.nist.gov/publications/safeguarding-international-science-research-security-framework.

[45] Office of the Director of National Intelligence. 2023. "Safeguarding Science." *Office of the Director of National Intelligence*. Retrieved on December 16, 2024 from www.dni.gov/index.php/safeguarding-science.

[46] Office of the Director of National Intelligence. 2023. *Foreign Collection and the Risk to U.S. Science and Technology: A Guide for Safeguarding Research and Innovation*. National Counterintelligence and Security Center. Retrieved on December 16, 2024 from www.dni.gov/files/NCSC/documents/SafeguardingScience/Foreign_Collection_8.5x11.pdf.

[47] Center for Development of Security Excellence (CDSE). 2023. "Foreign Collection Methods." *U.S. Department of Defense Security Awareness*. Retrieved on December 16, 2024 from https://securityawareness.usalearning.gov/cdse/multimedia/games/citrivia/foreigncollectionmethods.html.

[48] National Science Foundation. 2023. "Research Security." *National Science Foundation*. Retrieved on December 16, 2024 from https://new.nsf.gov/research-security.

As advanced research and technology development is also being conducted outside the traditional academic environment, a joint bulletin of 2024 has been issued by the Office of the Director of National Intelligence's National Counterintelligence and Security Center in cooperation with the Office of Economic Security and Emerging Technology, the Air Force Office of Special Investigations, and the Naval Criminal Investigative Service. The publication addresses the issue of protecting U.S. emerging technology companies from investment by foreign threat actors, with particular reference to China's government directives to invest in and acquire U.S. companies with the objective of obtaining technologies and intellectual property, and to facilitate technology transfer in support of the PRC state plans. The bulletin enumerates potential threat indicators, including complex ownership structures, investments through intermediaries, limited partner investments, requests for sensitive data, and exploitation of struggling U.S. firms. It also offers some guidance on risk mitigation and reporting.[49]

One of the key recommendations to reinforce the statutory framework is to modernize U.S. campaign finance, counter-interference, and espionage laws with the aim of enhancing transparency and disclosure requirements for individuals and entities acting on behalf of China. As proposed, this should include the implementation of more stringent sanctions and enforcement provisions to deter Chinese violators from interfering in the policymaking process, including issues of national security.[50]

One of the best examples to follow is the constant assessment and updating of risks and practices with a combination of leadership, from government bodies to professional associations.[51] An interdisciplinary team of experts has published a report on lessons learned from Red Teaming tabletop exercises on emerging technology proliferation threats. The report provides background information on five key lessons, including: 1. Lack of research security resources and culture at research institutions; 2. Low awareness of research collaborations with entities with links to defense end-users; 3. Foreign talent recruitment programs; 4. Lack of government outreach to vulnerable research institutions; and 5. Inadequate access controls to sensitive research, as well as highlighting individual and institutional best practice responses.[52]

The U.S. Department of State has made a formal declaration of its commitment to provide support to allies and partners in the protection of research and innovation. This is to be achieved through the promotion of openness, awareness and accountability.[53] For instance, the U.S. has invested in increasing awareness in the Baltics on different levels, including governmental. A briefing on the U.S.

---

[49] Office of the Director of National Intelligence. 2023. *Safeguarding Our Innovation: National Counterintelligence and Security Center Bulletin*. Retrieved on December 16, 2024 from www.odni.gov/files/NCSC/documents/products/FINALSafeguardingOurInnovationBulletin.pdf.

[50] Foundation for Defense of Democracies. 2024. *Cognitive Combat: China, Russia, and Iran's Information War Against Americans*. Retrieved on December 16, 2024 from www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf.

[51] Association of American Universities. 2020. *Effective Science Security Practices: Summary*. Retrieved on December 16, 2024 from www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf.

[52] University at Albany. 2024. *Threats and Best Practices in Research Security for Emerging Technologies: A Lessons Learned Report*. Retrieved on December 16, 2024 from www.albany.edu/cehc/cart#tab-publications.

[53] U.S. Department of State. 2023. "In Academia, Research Data is Sensitive: Here's How We Are Helping Reduce Security Risks." *U.S. Department of State*. Retrieved on December 16, 2024 from www.state.gov/in-academia-research-data-is-sensitive-heres-how-we-are-helping-reduce-security-risks.

- Baltics Multilateral engagement pointed to the increasingly competitive national security technical environment.[54]

2.2. European and other perspectives on the challenges of academic cooperation with China

2.2.1. Risk perception

A number of EU member states have acknowledged the reality of security threats embedded in intensified research cooperation with China. Already back in 2017, there was evidence that most of the academic collaborations between China and the EU28 have been mainly set up by Chinese researchers.[55] Other analysts have warned from 2016 to 2019 that there is significant evidence that the Chinese government, together with the Chinese military, private companies and unaffiliated citizens, will be conducting daily intrusions against major Western powers, as well as in the neighboring region, targeting academia, industry and government institutions for the purpose of collecting technological secrets, especially in cyber, 5G and data research.[56]

In 2019, transparency in academia was one of the measures recommended by the group of European experts in the "Handbook on Countering Russian and Chinese Interference in Europe" to increase accountability of those universities and research entities for the risks associated with cooperating with Chinese partners.[57] In 2020, a report by the Rhodium Group and the Mercator Institute for China Studies, while recognizing the many benefits of Sino-European R&D partnerships for Europe, also highlights some examples of cooperation that raise concerns due to security and human rights risks.[58] In 2020-21, interviewed government officials from Latvia and Estonia rated the risks of dependence on Chinese technologies as very high, weakening the countries' national resilience.[59] As of 2021, there were no comprehensive policies towards China in Latvia and Estonia in regards to opportunities and intersections between the states in security (i.e., information and cyber-security) and economics (i.e., trade and foreign direct investment) issues.[60]

---

[54] "U.S.–Baltics Multilateral Engagement," Ministry of Defence, Latvia. Accessed December 25, 2024. www.mod.gov.lv/sites/mod/files/document/U.S.%20%E2%80%93%20Baltics%20Multilateral%20Engagement.pdf.

[55] Wang, L., and Xianwen W. "Who Sets up the Bridge? Tracking Scientific Collaborations between China and the European Union." *Research Evaluation* 26, no. 2 (April 2017): 124–131. https://doi.org/10.1093/reseval/rvx009.

[56] Raud, M. *China and Cyber: Attitudes, Strategies, Organisation*. NATO CCDCOE, 2016. Retrieved on December 16, 2024 from https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf.
Kaska, K., Beckvard, H., and Minárik, T. *Huawei, 5G and China as a Security Threat*. NATO CCDCOE, 2019. Retrieved on December 16, 2024 from www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

[57] "Handbook on Countering Russian and Chinese Interference in Europe." *European Values*, 2020. Retrieved on December 16, 2024 from www.europeanvalues.cz/wp-content/uploads/2020/10/Handbook-on-Countering-Russian-and-Chinese-Interference-in-Europe.pdf.

[58] "MERICS-Rhodium Group COFDI-Update-2020." *MERICS*, May 2020. Retrieved on December 16, 2024 from www.merics.org/sites/default/files/2020-05/MERICS-Rhodium%20Group_COFDI-Update-2020_3.pdf.

[59] Teperik, D., et al. "Resilience Against Disinformation: A New Baltic Way to Follow?" *International Centre for Defence and Security*, Tallinn, Estonia, 2022. http://dx.doi.org/10.13140/RG.2.2.29369.44649.

[60] "China, Central and Eastern Europe." *Taylor & Francis*, accessed December 25, 2024. www.taylorfrancis.com/chapters/edit/10.4324/9781003096948-11/china-central-eastern-europe-aleksandra-kuczy%C5%84ska-zonik-tomasz-st%C4%99pniewski.

In the 2024 study, "EU-China relations: De-risking or de-coupling − the future of the EU strategy towards China", which was requested by the European Parliament Committee on Foreign Affairs, the authors identified several challenges for future research, education and people-to-people cooperation between EU countries and China. Should the current imbalance in research collaboration persist, it is possible that China's economic development may benefit more than the EU's interests, thereby contributing to China's technological advancement. As previously noted, the Chinese Party-State exerts considerably more control over those engaged in academic exchanges than the EU does. Furthermore, numerous semi-autonomous organizations in China have witnessed a tightening of state control over the past decade, including in academia. Chinese intelligence has been known to utilize employment opportunities in EU academia and think tanks as a means of obtaining intelligence. Nevertheless, the authors also suggest that the design of risk-mitigating policies should consider seeking a balance between potential risks and benefits. It would be erroneous and counterproductive for the EU to automatically consider Chinese researchers as agents of the Chinese state. It is in the EU's interest to sustain and even deepen people-to-people exchanges with China, including research collaboration.[61]

A number of experts have argued that there is no need for the EU to impose strict limitations on academic cooperation with China. They contend that even research in sensitive areas that may be perceived as high-risk could, in fact, be beneficial to the EU and in line with its best interests. They further argue that implementing additional controls on research collaboration between China and the EU would prevent researchers from engaging closely with each other. Indeed, there has been mounting pressure to effectively halt any research collaboration with Chinese counterparts, even in the absence of clear legal requirements and frameworks.[62] A recent case of several European universities cooperating with Chinese entities linked to the PLA was quite resonating, as the universities were aware of the risks but decided to proceed as the research project's topic was not that controversial.[63]

2.2.2. Policies and practices of risk mitigation

The general number of various check-lists and knowledge security-oriented documents in Europe is increasing. Adopted by the Council of the European Union in 2023, "The Recommendations on The European Framework to Attract and Retain Research, Innovation and Entrepreneurial Talents in Europe" include a paragraph on knowledge security as follows: "Given the increasing focus on knowledge security, researchers should always adopt safe working practices, in line with relevant national and Union legislation, including taking the necessary precautions for health and safety and for recovery from cybersecurity attacks, and information technology disasters, e.g. by preparing proper back-up strategies. They should also be familiar with the current national and Union legal requirements

[61] "Council Adopts a Recommendation to Enhance Research Security." *Council of the European Union*, May 23, 2024. Retrieved on December 16, 2024 from www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security.

[62] "Strict Ban on China Will Cost Us Dearly in Science." *Clingendael Institute*. Accessed December 25, 2024. www.clingendael.org/publication/strict-ban-china-will-cost-us-dearly-science.
"Research Collaboration: Drawing Red Lines with China Isn't Easy." *MERICS*. Accessed December 25, 2024. https://merics.org/en/comment/research-collaboration-drawing-red-lines-china-isnt-easy.

[63] "Europe Teams Up with Universities Linked to China's Military." *Politico*. Accessed December 25, 2024. www.politico.eu/newsletter/china-watcher/europe-teams-up-with-universities-linked-to-chinas-military.

regarding data protection and confidentiality protection requirements and undertake the necessary steps to always fulfil them."[64]

While generally, risk mitigation could be solved on the national level, the European Commission came up with the staff working document on Tackling Research and Innovation (R&I). The document serves as a comprehensive strategy for Higher Education Institutions and Research Performing Organizations. The EC approach, as a starting point (as a first point of orientation), selects the Academic Freedom Index. The basis of the document is protection of academic freedom. For instance, it contains the following guidance: "Continue to cooperate with partners in repressive settings. Avoid stigmatizing or alienating students, academic colleagues and institutions in non-liberal institutional environments."[65]

With emphasizing values, norms and decisions, the European Commission defines foreign interference with a focus on the cognitive domain (however, not naming it as such). While mentioning the main objectives to further political, socio-cultural, economic, and technological interests of the foreign actor, the document also listed: "to unlawfully retrieve information of interest to the foreign actor; to influence decisions in favor of the foreign actor, to undermine values perceived as contrary to the foreign actor." Also, among techniques used by the potential influencers are cognitive domain tailored activities. The document does not mention China; however, the awareness raising procedures could be easily connected to the framework referred to in the first part of the literature overview.

A recent report, entitled "National Perspectives on Europe's De-risking from China", was published by the European Think-tank Network on China in 2024. The report provides a concise overview of the China-related risks and de-risking measures in 22 European countries, including Latvia but not Estonia. As indicated in the report, discourses on de-risking in the EU are frequently situated within broader discussions on economic security. Furthermore, there are notable differences between the national strategies employed by European countries in addressing China-related risks. In the case of Latvia, the absence of de-risking narratives is highlighted, which can be attributed to the country's minimal dependence on China or the lack of political prioritization of this issue. With regard to the domain of research security, several of the surveyed countries have demonstrated a focus on knowledge and technology transfer in their policy debates and respective measures related to academic collaboration. However, this aspect has not been a prominent feature in Latvia's policy debates.[66]

In 2024, the European Commission published a proposal for a Council Recommendation on enhancing research security. The proposal also is based on academic freedom and institutional autonomy. Among other recommendations, the Commission recommends establishing the European Centre of Expertise on Research Security "as a focal point, linked to the Commission's one-stop platform on tackling R&I foreign interference, contributing to creating an EU-wide community of practice and maintain a structural dialogue with stakeholder organizations as well as to policy-relevant research into research security and analyzing trends and patterns across the Union." The recommendations were adopted in May 2024 and offer guidance for measures that could be taken by

---

[64] "Commission Implementing Decision (EU) 2023/1640 of 10 August 2023 on the Adoption of the List of Critical Technologies." *EUR-Lex*. Accessed December 25, 2024. https://eur-lex.europa.eu/eli/C/2023/1640/oj.

[65] European Union. *Tackling R&I foreign interference*. Directorate-General for Research and Innovation (European Commission), 2022. Accessed December 25, 2024. https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1.

[66] "National Perspectives on Europe's De-risking from China." *MERICS*, June 2024. Retrieved on December 16, 2024 from https://merics.org/sites/default/files/2024-06/ETNC%202024_National%20Perspectives%20on%20Europe%E2%80%99s%20De-risking%20from%20China_FINAL_low.pdf.

the European Commission, the member states and the research community. The next report of monitoring is projected for mid-2025.[67]

In accordance with the recommendations of the authors of the study commissioned by the European Parliament's Committee, the EU should adopt a de-risking policy that targets precisely those forms of academic and research exchange and cooperation that pose risks, while not placing any restrictions or undue burden on the majority of forms of engagement and cooperation that pose no threat and remain important for sustaining bilateral relations as well as improving European competitiveness.[68]

In February 2024, the Security and Integrity of the Global Research Ecosystem Working Group endorsed the "Best Practices for Research Security & Integrity", which includes four main directions. It is recommended that resources be established to promote awareness and forums for dialogue and information sharing on research security and integrity across all research stakeholders. In addition, it is necessary to identify and share information on which research areas are at risk. Furthermore, it is important to identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information. Finally, it is essential to implement risk mitigation measures, both as standard organizational practice and for individual research projects.[69]

As recommended, it is imperative that governments acknowledge the inherent risks associated with collaboration with China. Scientists, on the other hand, must recognize that research collaborations are not conducted in isolation and that government intervention is therefore necessary. Effective risk management in research collaboration with China will necessitate coordination and collaboration not only between EU countries but also with the UK and other allies. Additionally, effective screening and oversight must be sensitive and implemented on a case-by-case basis in close cooperation with individual institutions.[70]

On the other hand, some policy analysts proposed more proactive measures for the adoption of actor-agnostic regulations to safeguard trusted research and knowledge security. These included the definitions of sensitive areas, governmental assistance to HEIs in developing and applying useful mechanisms to evaluate the potential risks to research integrity (risk matrix), the designation of a National Contact Point for Knowledge Security, and so forth.[71]

Furthermore, a number of countries have enacted their own regulatory frameworks. As suggested to HEIs in the Swedish Guidelines for reflection on international academic collaboration, "for some collaborations, intellectual property issues may need to be assessed, while other projects need to be considered in relation to non-disclosure agreements, national security issues and sanctions. Sometimes

---

[67] "Council Adopts a Recommendation to Enhance Research Security." *Council of the European Union*, May 23, 2024. Retrieved on December 16, 2024 from www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security.

[68] European Parliament Think Tank. *EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China.* Accessed December 25, 2024. www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2024)754446.

[69] "G7 Best Practices for Secure and Open Research." *Science.gc.ca.* Accessed December 25, 2024. https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research.

[70] Clingendael Institute. *Strict Ban on China Will Cost Us Dearly in Science.* Accessed December 25, 2024. www.clingendael.org/publication/strict-ban-china-will-cost-us-dearly-science.
MERICS. *Research Collaboration: Drawing Red Lines – China Isn't Easy.* Accessed December 25, 2024. https://merics.org/en/comment/research-collaboration-drawing-red-lines-china-isnt-easy.

[71] JCU. *How to Do Trusted Research.* Accessed December 25, 2024. www.jcu.cz/images/veda-a-vyzkum/dokumenty-vav/htdtr_report_how-to-do-trusted-research_a4_16_web.pdf.

a media risk assessment is conducted and financial risk assessments may also occur. Therefore, certain preliminary assessments of collaborative projects are currently already being conducted."[72]

The United Kingdom's Government has developed the "Research and Innovation Trusted Research and Innovation Principles," which include references to recommendations for UK universities on managing risks in internationalization and guidelines on security-related issues (e.g., sensitive research material, academic technology approval scheme, etc.).[73] In addition, launched by Universities UK in 2019, Trusted Research has evolved into a partnership with the UK's National Protective Security Authority and the National Cyber Security Centre, working together to produce practical guidance for academics on protection frameworks and risk mitigation approaches in universities and research institutions.[74]

In 2022, the Ministry of Education and Culture of Finland published recommendations for academic cooperation with China, which were prepared in collaboration with Finnish HEIs and research institutes, as well as their key stakeholders. The document provides a valuable example of the issues to consider for Latvian and Estonian academia.[75]

It is also recommended that the Australian Government's "Guide to Intellectual Property in Research Collaborations in China" be consulted, as it provides a wealth of useful information on this topic. The Australian Government has a well-established tradition and significant experience in countering Chinese threats in various areas, including the academic sector.[76]

Canada's "Guidelines and Tools to Implement Research Security: National Security Guidelines for Research Partnerships" offers a valuable source of inspiration for Baltic academia, as it is based on comprehensive documents that include the Policy on Sensitive Technology Research and Affiliations of Concern, Guidance on Conducting Open Source Due Diligence Guidance for Research Organizations, Funders, and Universities. Furthermore, the framework offers case studies on scenarios and emerging technology trend cards. Canada's approach recommends the establishment of research security centers to facilitate more accurate risk profile assessments and more efficient risk mitigation strategies.[77]

In accordance with Canada's Policy on Sensitive Technology Research and Affiliations of Concern, researchers are obliged to review the list of Named Research Organizations where entities from China and Russia can be found, as the list comprises research organizations and institutions that present the

[72] STINT. *Responsible Internationalisation.* Accessed December 25, 2024. www.stint.se/wp-content/uploads/2020/02/STINT__Responsible_Internationalisation.pdf.
[73] UK Research and Innovation. *Trusted Research and Innovation Principles.* Accessed December 25, 2024. www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf.
[74] National Protective Security Authority. *Trusted Research Academia.* Accessed December 25, 2024. www.npsa.gov.uk/trusted-research-academia.
[75] Finnish Ministry of Education and Culture. *OKM 2022/11.* Accessed December 25, 2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163963/OKM_2022_11.pdf.
[76] IP Australia. *Guide to Research Collaboration in China.* Accessed December 25, 2024. https://beta.ipaustralia.gov.au/international-ip/how-to-apply-for-ip-overseas/ip-in-china/~/-/media/Project/IPA/IPAustralia/PDF/guide-research-collaboration-in-china.pdf?rev=58b77e76c6fb4c458fd23098536aa1df.
[77] Government of Canada. *Guidelines and Tools for Implementing Research Security.* Accessed December 25, 2024. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security.

greatest risk to Canada's national security due to their direct or indirect connections with military, national defense, and state security entities.[78]

Lastly, the "Checklist for Collaboration with Chinese Universities and Other Research Institutions" published by the Hague Centre for Strategic Studies can serve as another good example of an institutional approach to addressing knowledge security issues.[79]

Given the complexity of existing and emerging security challenges and influencing factors, as well as the local or regional contexts, the question arises as to how prepared the Baltic states of Latvia and Estonia are today to identify threats of Chinese influence activities and to mitigate the risks in different areas, especially in the field of academia and international scientific cooperation.

2.3. China-related threat awareness in Latvia and Estonia

Influence activities of China in Latvia and Estonia have been recognized as security threats during the past five to seven years. This awareness process has been mostly driven by national intelligence and internal security agencies whose annual reviews have warned the publics about rising China's espionage, cyber interference and other malicious influence actions in various sectors, foremost business investments, infrastructure, and critical technologies. The risks of interactions with China have been analyzed through the prism of national security focusing mostly on increasing the protection of government agencies and their officials as well as rising awareness regarding the vulnerabilities of 5G and other technologies which might be directly or covertly controlled by China. Some researchers point out that the footprints of Chinese influence activities in Latvia and Estonia are quite similar, but each country has its own specificities.[80]

Historically, awareness about China-related threats in Latvia and Estonia has been based on information provided by state intelligence and counterintelligence agencies in their annual reviews. According to the Estonian Internal Security Service, the interests of China address both government-forced technology transfer and civil-military cooperation programs that involve communities, researchers, technology firms or Chinese trade chambers established abroad. China's intelligence objectives are supported by various laws that compel both Chinese citizens and businesses to cooperate extensively with state structures. The case of the recruitment of two Estonian citizens by China's military intelligence demonstrates the interest in research data, as their methods can also include targeting individuals with no prior ties to China but who possess valuable expert knowledge.[81] The Estonian Foreign Intelligence Service has warned that the spread of Chinese technology into critical infrastructure, such as energy grids, poses a threat to Estonia's security.[82]

---

[78] Government of Canada. *Sensitive Technology Research and Affiliations of Concern*. Accessed December 25, 2024. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations.

[79] "Checklist for Collaboration with Chinese Universities and Other Research Institutions." *HCSS*, Accessed December 25, 2024. https://hcss.nl/report/checklist-for-collaboration-with-chinese-universities-and-other-research-institutions.

[80] Kolomaznik, T. "Baltic States: From Pragmatism to Cooling of Relations." In The Dragon at the Gates of Europe: Chinese Presence in the Balkans and Central-Eastern Europe, edited by Andrea Bogoni and Brian F. G. Fabrègue, 377–396. Blue Europe, December 2023. Retrieved on December 16, 2024 from www.blue-europe.eu/analysis-en/short-analysis/baltic-states-from-pragmatism-to-cooling-of-relations.

[81] "Annual Review 2023–2024." *Estonian Internal Security Service*, 2024. Retrieved on December 16, 2024 from https://kapo.ee/sites/default/files/content_page_attachments/Annual%20review%202023-2024.pdf.

[82] Estonian Foreign Intelligence Service. *Annual Report 2024*. Accessed December 25, 2024. https://valisluureamet.ee/doc/raport/2024-en.pdf.

In its 2023 annual report, Latvia's Constitution Protection Bureau (SAB) has devoted a separate subsection to China-related threats in research and academia. The SAB highlights the following risks of cooperation with China: Chinese nationals are subject to state control, as they can be forced to report on their activities and results; and share jointly developed technologies and acquired knowledge that can serve China's strategic interests, especially military and technological development in areas where China has shown increased interest and invested resources: biotechnology, artificial intelligence, quantum technology, green energy. China is seeking to establish dominance through the development of emerging and disruptive technologies to secure unique opportunities to achieve absolute advantage in a particular sector, to create a new market and to control it.[83]

To advance China's strategic vision, as researched by several Latvian and Estonian scholars, the objectives of China include the creation and maintenance of a positive image among decision-makers and agenda-setters in Latvia and Estonia. Naturally their target audiences include politicians, government officials and business leaders. In addition, opinion leaders from other sectors, including academia can be considered by China as worthy to shape their attitudes and nudge them in favor of endorsing more interaction between their institutions and Chinese counterparts.

In their overview of "Societal Security in the Baltic Sea Region," the Latvian and Estonian authors do not mention knowledge security or research operational security specifically. However, they do acknowledge the role of academia and think tanks as major stakeholders in societal resilience.[84] As indicated in the report, "China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden" by the NATO Strategic Communications Centre of Excellence, academic relations may be one of the areas in which China exerts the greatest influence, in comparison to other sectors in the region.[85]

There are few studies in Latvia and Estonia that assess malicious implications of academic and research cooperation with Chinese universities and scientific institutes. Accordingly, research and teaching staff in Latvian and Estonian universities and institutions might be not fully aware of the incoming China-related threats nor properly equipped to manage them. Nevertheless, there are some significant cases that illustrate the seriousness of the problem. For example, an Estonian investigative journalist, H. Roonemaa, published an article claiming that a Chinese influence agent had been working in several Estonian universities for years.[86] The Baltic Centre for Investigative Journalism (Re:Baltica) has published an article on the role of the Confucius Institute in advancing China's influence through educational propaganda in Latvia.[87]

The 2022 joint publication, "China in the Baltic States – from a cause of hope to anxiety," provides a comprehensive overview of the perception and role of China in Latvia, Estonia, and Lithuania. The publication emphasizes the implications of China's presence in the region for the national security of

[83] Latvian Security Police. *SAB Annual Report 2023*. February 2024. Retrieved on December 16, 2024 from www.sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_ENG.pdf.
[84] "Societal Security in the Baltic Sea Region: Expertise Mapping and Raising Policy Relevance." *Latvian Institute of International Affairs*, accessed December 25, 2024. https://liia.lv/en/publications/societal-security-in-the-baltic-sea-region-expertise-mapping-and-raising-policy-relevance-716?get_file=1.
[85] NATO StratComCOE. "China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden". Accessed December 25, 2024. https://stratcomcoe.org/publications/chinas-influence-in-the-nordic-baltic-information-environment-latvia-and-sweden-full-report/239.
[86] "Varjatud leid KAPO aastaraamatust: Eesti ülikoolides kõrgetel kohtadel töötanud mees on Hiina mõjuagent." *Eesti Päevaleht*, September 9, 2020. Retrieved on December 16, 2024 from https://epl.delfi.ee/artikkel/96618779/varjatud-leid-kapo-aastaraamatust-eesti-ulikoolides-korgetel-kohtadel-tootanud-mees-on-hiina-mojuagent.
[87] Rebaltica. "Hiina pehme võimu räpane nägu." *Rebaltica*, August 2019. Retrieved on December 16, 2024 from https://rebaltica.lv/2019/08/kinas-maigas-varas-rupja-seja.

the three Baltic states. As the authors posit, the rise of China as a media, policy, and security topic is a consequence of Chinese presence in the region and a reflection of broader global trends and circular and bilateral interdependencies, including in research and technology domains.[88]

The analysis, entitled "The Asymmetry of Estonian-Chinese Relations, Research Cooperation and Indirect Threat," was published by the International Centre for Defence and Security (Estonia) in February 2024. It focuses on bilateral academic cooperation on dual-use technologies in the field of technology transfer, highlighting some joint research publications. The general assumption is that indirect benefits of research cooperation can unintentionally contribute to the development of China's military industry sector. The analysis posits that there is a low intensity of research cooperation between Estonia and China. However, it identifies areas of Chinese interest in which Estonia has some comparative advantage, including cyber, detection technologies and materials science. The analysis recommends the implementation of preventive measures, such as limiting access to sensitive information, to gain an understanding of China's interests, objectives, and laws. This would enable the creation of a framework for the assessment of the risks associated with research cooperation.[89]

In the recent article "Mapping the Scope of China's Soft Power in Estonia", the authors conclude that the primary sources of China's soft power – namely its traditional culture, success in science and technology development, and grand foreign policy initiatives – are present in Estonia. Furthermore, they note that most research cooperation between China and Estonia occurs at the university level.[90]

F. Jüris in his recent publication "Making friends, making inroads: the CCP's influence activities in Estonia" provides a comprehensive overview of the CCP's United Front and propaganda work, as well as the variety of forms it takes in its interactions with different target groups, including academia.[91]

The authors of the analysis "The People's Republic of China in the Baltic States" looked at the relations through the prism of dependency and conditionality in main categories, and noted that some changes regarding cooperation with China can be observed in academic circles in Latvia and Estonia, as several long-term practices (e.g. educational exchanges and research mobility) have been questioned, and it has been an eye-opener for researchers and teaching staff.[92]

In 2023, the University of Tartu (Estonia) conducted a study with the objective of providing insight into Estonians' attitudes towards China. The findings of the study can inform decision-making in the short and long term regarding the economy, security, education, and culture. The study aimed to inform the development of strategies to respond to Chinese influence operations, to plan China-related education and cultural policies, and to maximize the economic benefits for Estonian society. The study's findings indicate that the sentiment of Estonia's allies towards China has become significantly more hostile in recent years, as evidenced by the opinions of the populations of developed

[88] Riga Stradiņš University. "China in the Baltic States: From a Cause of Hope to Anxiety." Accessed December 25, 2024. www.rsu.lv/sites/default/files/imce/Projekti/Da%C5%BE%C4%81di/china-in-the-baltic-states-from-a-cause-of-hope-to-anxiety.pdf.

[89] Kuusepaik, Heli. *Eesti-Hiina Suhete Asümmeetrilisus: Teaduskoostöö ja Kaudne Oht. International Centre for Defence and Security*, February 2024. Retrieved on December 16, 2024 from https://icds.ee/wp-content/uploads/dlm_uploads/2024/02/RKK_Analuus_Eesti-Hiina_Suhete_Asummeetrilisus_Teaduskoostoo_ja_Kaudne_Oht_Heli_Kuusepaik_Veebruar_2024.pdf.

[90] World Scientific. "People's Republic of China in the Baltic States." *World Scientific*, 2023. Retrieved on December 16, 2024 from www.worldscientific.com/doi/epdf/10.1142/S1793930523000272.

[91] Jüris, F. "The CCP's Influence in Estonia." *Sinopsis*, August 2023. Retrieved on December 16, 2024 from https://sinopsis.cz/wp-content/uploads/2023/08/ccpestonia0.pdf.

[92] "People's Republic of China in the Baltic States." *Riga Stradiņš University*, Accessed December 25, 2024. https://science.rsu.lv/files/57925209/peoples_republic_of_china_in_the_baltic_states_1075.pdf.

Western countries. Nevertheless, there is a strong recognition in Estonia that cooperation with China is necessary. Indeed, there were few respondents who did not consider cooperation with China necessary in any area. As perceived by Estonians, the areas in which cooperation with China is most commonly seen are economic, scientific, cultural and climate related.[93]

The Central European Institute of Asian Studies has published a map of 11 European countries (as of April 2024) where interactions between European academic institutions and Chinese entities have been identified.[94] The map is based on data collected from various open sources, with the methodology initially comprising the gathering of data through Freedom of Information Act requests to public universities and research institutes. The project did not cover Estonia, but seven Latvian higher education institutions provided data about academic cooperation with Chinese partners. Riga Technical University reported 20 academic interactions with counterparts from China, while the University of Latvia reported 12. It should be noted that some of the Chinese institutions are linked to the People's Liberation Army by the Australian Strategic Policy Institute's China Defense University Tracker. As studied by K. Andrijauskas, Latvian and Estonian top universities have signed bilateral cooperation agreements with Chinese counterparts listed in the ASPI China Defense Universities Tracker (2021), including top secret and very high-risk institutions.[95]

Latvian scholars O. Nikers and O. Tabuns, in their publication "Between Brussels and Beijing: The Transatlantic Response to the Chinese Presence in the Baltic Sea Region," argue that China relies on education and research links, including China's public diplomacy and state-sponsored language education, because the combination of European academic freedom and science funding issues, in particular, provide low-hanging fruit for Beijing to achieve several goals at once.[96] As cited in the publication "Latvia external relations briefing: Developments, Policies, and Prospects of Latvia's Relations with China" by the China-CEE Institute, "the prospects for cultural and educational exchanges between Latvia and China appear promising". This is just one of the evidenced examples by the indication of China's attempts to influence perceptions within Latvian academia.[97]

In the Latvia and Estonia chapters of the publication "State of play of academic freedom in the EU Member States: Overview of de facto trends and developments," no concerns were explicitly expressed regarding cooperation with China-related academic entities or universities. However, it is notable that in other countries, such as Germany, Cyprus, and China, Confucius Centers play a role in fostering self-censorship related to China. This is particularly evident in the lack of transparency surrounding the funding of these centers, which raises questions about the extent to which this funding leads to self-censorship. Furthermore, in Finland, guidelines for academic cooperation with

[93] "Eestimaalaste Hiina hoiakute uuring. " *University of Tartu*, Accessed December 25, 2024. https://aasiakeskus.ut.ee/et/media/44770/download?attachment.
[94] Academy Tracker. "EU-China Research Collaboration." Accessed December 25, 2024. https://academytracker.ceias.eu/map/eu.
[95] Andrijauskas, K. "Baltic Security and Chinese Influence." *Journal on Baltic Security*, Accessed December 25, 2024. https://journalonbalticsecurity.com/journal/JOBS/article/7/file/pdf.
[96] Nikers, O. and Tabuns. O. "Between Brussels and Beijing: The Transatlantic Response to the Chinese Presence in the Baltic Sea Region." *Jamestown Foundation*, Accessed December 25, 2024. https://jamestown.org/product/now-available-between-brussels-and-beijing-the-transatlantic-response-to-the-chinese-presence-in-the-baltic-sea-region/.
[97] China-CEE Institute. "Latvia: External Relations Briefing—Developments, Policies, and Prospects of Latvia's Relations with China." *China-CEE Institute*, March 22, 2024. Retrieved on December 16, 2024 from https://china-cee.eu/2024/03/22/latvia-external-relations-briefing-developments-policies-and-prospects-of-latvias-relations-with-china/.

China were published in December of last year by the Ministry of Education and Culture, based on advice from the Finnish Security Intelligence Service.[98]

Nevertheless, as concluded by Dr U. A. Bērziņa-Čerenkova from the Latvian Institute of International Affairs in her short overview, "Carelessness Rooted in Low Threat Perception," there are no significant risks or dependencies to Latvian universities resulting from academic collaboration with China.[99] In 2019, Dr Bērziņa-Čerenkova co-authored a NATO StratCom COE report "Hybrid Threats: Confucius Institutes".[100] The first finding listed as a key point in the executive summary stated that "Institutions like these should not automatically be viewed as hostile." However, other Latvian and Estonian researchers agree that one of the most powerful instruments of China-related soft power and influence is the Confucius Institute, which has almost monopolized the teaching of the Chinese language and the mediation of official cultural and academic relations between China, and Latvian and Estonian universities.

In 2021, Dr Bērziņa-Čerenkova conducted an analysis of the principal risks associated with increased Chinese involvement in Latvia and Estonia. In addition, she has compared the countries' resilience along three intertwining domains: systemic, discursive, and financial. She concluded that both countries have the systemic resilience to withstand external pressures. This is due to a number of factors, including anti-authoritarian sentiment due to the domestic interwar historical background, Euro-optimism due to the lack of political autonomy and economic development during the Soviet occupation period, and pro-Atlanticism due to the deterring role of NATO vis-à-vis Russia in the region. Furthermore, the case of Latvia and Estonia demonstrates that it is possible to engage in a pragmatic dialogue with China without subscribing to its discourse on political values and remaining loyal to the EU value outlook.[101]

Another recent report, "Classic Cleavages in a New Light: Chinese Informational Influence in the Baltics," written jointly by five Baltic authors, has assessed the susceptibility and resilience of the societies of the three Baltic states to Chinese influence in the information domain. Public perceptions on China-related threats in Latvia and Estonia can be characterized in general as ambiguous, as there is an evident tendency to separate economic questions from political issues. More than half of Latvian and Estonian respondents think that having good relations with China is economically and politically beneficial. Notably, 52% of Latvians and 40% of Estonians share the opinion that Chinese students should have all possibilities to study in their country.[102]

Latvian and Estonian academia can benefit from studying Taiwan's experience in countering the Chinese co-optation tactics when recruiting politicians, businessmen, academics, media influencers,

---

[98] European Parliament. "Research Collaboration with China: Policy Developments." *European Parliament*, December 2023. Retrieved on December 16, 2024 from www.europarl.europa.eu/RegData/etudes/STUD/2023/740231/EPRS_STU(2023)740231_EN.pdf.

[99] "Articles and Analysis on EU-China Research Collaboration." *Academy Tracker*, Accessed December 25, 2024. https://academytracker.ceias.eu/articles/68NLHnYpNmyNW5iF5SpDxK.

[100] NATO StratComCOE. "Hybrid Threats: Confucius Institutes." *NATO StratCom Centre of Excellence*, 2024. Retrieved on December 16, 2024 from https://stratcomcoe.org/publications/download/confucius_institutes.pdf.

[101] Berzina-Cerenkova, U.-A. "The Baltic Resilience to China's Divide and Rule." *Lex Portus* 7, no. 2 (2021): 11–38. https://doi.org/10.26886/2524-101X.7.2.2021.2.

[102] Merkinaitė, S. *et al. Classic Cleavages in a New Light: Chinese Informational Influence in the Baltics.* Vilnius: Eastern Europe Studies Centre, 2024. Retrieved on December 16, 2024 from www.eesc.lt/en/publication/classic-cleavages-in-a-new-light-chinese-informational-influence-in-the-baltics.

and entertainers by providing all-expenses-paid trips to China where recruitment or indoctrination can be attempted, including proposals for some positions in Chinese universities or research centers.[103]

In the 2022 publication "How to Do Trusted Research: China-Specific Guidelines for European Stakeholders" by the Association for International Affairs, neither Latvia nor Estonia were identified as European countries that have adopted trusted research guidelines applicable to cooperation with China-associated academic entities.[104]

Given the background of Latvia's and Estonia's relations with China, as well as the evolving security situation in the region, it seems feasible to assess the existence and effectiveness of policy frameworks and guiding practices within Latvian and Estonian academia and government agencies to mitigate risks arising from research cooperation with China and to minimize potential threats associated with Chinese malicious intentions.

Prior to presenting the empirical findings of the situational analysis in Latvia and Estonia, the summary of both sections can be provided with a quotation from the foreword to the "Global Engagement: Rethinking risk in the research enterprise", where H.R. McMaster, former National Security Adviser, a retired U.S. Army lieutenant general, wrote that the basic steps proposed for addressing the problem set – namely, knowing one's funders, taking contracts seriously, training, iterating, and adapting – have relevance beyond research institutions.[105]

In light of the identified gaps in the available research on the two Baltic countries, the following chapter addresses ongoing efforts in government-academia collaboration to raise awareness of risk mitigation in Latvia and Estonia.

[103] Baltic Defence College. *Hybrid Threats*. Latvia: LIIA, 2024. Retrieved on December 16, 2024 from www.baltdefcol.org/files/files/publications/Hybrid%20Threats_LIIA.pdf.
[104] JCU. *How to Do Trusted Research*. Czech Republic: JCU, 2016. Retrieved on December 16, 2024 from www.jcu.cz/images/veda-a-vyzkum/dokumenty-vav/htdtr_report_how-to-do-trusted-research_a4_16_web.pdf.
[105] McMaster, H. R. "Foreword." In *Global Engagement: Rethinking Risk in the Research Enterprise*, edited by Glenn Tiffert. Hoover Institution Press, 2020.

3. FINDINGS ON THE STATE OF RESEARCH SECURITY IN LATVIA AND ESTONIA

The general methodology of the empirical research was based on conducting desk research and semi-structured in-depth interviews with representatives of major universities and research institutions, as well as government officials responsible for research strategy and policies, including international academic cooperation. Additionally, some experts on China and national security were included in order to provide their assessment of possible threats to academia in Latvia and Estonia.

The interviews were conducted from May to July 2024. The collected data was anonymized and subsequently structured and analyzed in accordance with the following research questions[106]:

- How intensive has academic and/or research cooperation been with China during the recent 10-12 years?
- How sufficient is threat awareness about possible foreign interference and dangers related to cooperation with China and other authoritarian states at the national, institutional and individual level?
- Are there established procedures (protocols, trained staff) to assess security risks associated with cooperation with China applied at national and/or institutional and/or individual levels?
- What measures should be recommended in order to increase the level of operational security within academia?

The following public and empirical findings are presented separately for each country's sector, given the existence of national differences and institutional nuances, including the scales and optics of threat perception and mitigation measures.

3.1. Case of Latvia

As previously mentioned, in the 2023 annual reports of the Internal and Foreign Intelligence services, for the first time, risks to academia and science were noted. As indicated in an interview by a representative of Latvia's Constitution Protection Bureau, the risks are increasing from day to day, so there is an intensification in activities to raise awareness.

Raising awareness and protection requires a comprehensive approach, including different types of public discourse, especially taking into account recent conflicting messages. The official Latvian discourse on China is changing. Almost a decade ago, as mentioned by the majority of respondents from the academic and government sectors, the leading message was to strengthen different types of partnerships, including academic and research partnerships.

Latvia's position towards partnerships with China could be observed in the "Annual Report of the Minister of Foreign Affairs on the Accomplishment and Further Work With the Respect to National Policy and the European Union." Within the last few years, the discourse of partnerships, with a peak in 2016[107], was overshadowed by increasing cooperation between China and Russia.

[106] Please find the full list of questions asked during the in-depth interviews in the attached annex.

[107] In the report of 2016-17, Latvia's primary interests were set as the "development of cooperation in transport and logistics sector with a view to achieving a regular flow of transit cargos from China and launching direct flights. In the

In 2021, Latvia devoted greater attention to the dialogue between the European Union and China, as well as bilateral relations with China by correlating the involvement in the "16+1" format events with Latvia's interests in the specific field. Seeking to promote the European Union's unity in relations with China, Latvia is standing up for the development of cooperation by all the European Union Member States in a common "27+1" format."[108] At the same time, the minister mentioned increasing Russia and China coordination.

In January 2024, the Minister of Foreign Affairs Krišjānis Kariņš addressed the parliament regarding national foreign policy. He said," China is a topic that has recently been appearing more often, especially in the press, and people ask: what is the position and attitude of our country? Is China a partner? Is China a threat? Is China an opportunity? And the answer is, all those things."[109] He called the former governmental policy regarding China (2016-2017) "naive". Kariņš continued, "It is a fact that China is heavily involved in global supply chains, a lot of items that we use on a daily basis, or their components come from China. Whether we want it or not, it is a fact. The main point is – not to create a new dependency. Do not create a new dependency!"[110] He said, "We also need to keep our eyes open for risks, including in terms of technology."[111]

Representatives of the foreign security services use a variety of formal and informal formats to inform the public about the increasing risks and suggest ways to mitigate them. For the academic sector, the shift from promoting foreign cooperation, including with China, to the protection of national security is controversial.

Limitations in closer cooperation with the national security apparatus were identified based on interviews with both the representatives of the academic sector and representatives of the security sector, including stigma on the work of security services, coming from the Soviet past and threats to academic freedom. Other identified gaps included lack of a systematic approach to collect needed data and control (internally) foreign interventions in academia and research institutions; lack of resources (human and financial), as well as lack of platforms and channels for communication to increase awareness of risks from foreign interventions. Regarding private academia and research, it is crucial not to leave them aside.

3.1.1. Latvian research institutions awareness

It is the Law on Scientific Activity that regulates interactions with foreign researchers, defines protection of the Property Rights and serves as a main document referred to by interviewed

talks, a major emphasis was placed on potential cooperation with China in the tourism sector, and consequently, work has been started on a strategy to attract Chinese tourists. Certification of the manufacturers of a number of Latvian food and plant products can be regarded as one of the current tangible benefits from Latvia's cooperation with China in the "16+1" format.

[108] Ministry of Foreign Affairs of Latvia. *Speech by Foreign Minister Krisjānis Kariņš at the Annual Foreign Policy Debate in the Latvian Parliament, Saeima, January 25, 2024*. Retrieved on December 16, 2024 from www.mfa.gov.lv/en/speech-foreign-minister-krisjanis-karins-annual-foreign-policy-debate-latvian-parliament-saeima-25-january-2024.

[109] Ministry of Foreign Affairs of Latvia. *Annual Foreign Policy Report*. 2024. Retrieved on December 16, 2024 from www.mfa.gov.lv/en/media/5240/download?attachment.

[110] *Ibid.*

[111] *Ibid.*

representatives from academia and government institutions in Latvia.[112] Other relevant regulations include the Law On the Circulation of Goods of Strategic Significance and others.

The National Scientific Activity Information System (Science Latvia) provides annual public reporting from research entities, also making transparent partnerships with foreign entities.[113] Private institutions, as could be observed on the portal, are skipping public reporting.

Latvia registered scientific institutions are contributing to both national and international science. There are numerous projects registered in the data sets that are available. However, while data collection is an important element of monitoring, the quantity and quality of information in reporting identify possible gaps that should be addressed in the further mitigation of risks to national and international research integrity. This applies also to partnerships with Latvia registered organizations which have connections with foreign headquarters in non-democratic countries. This knowledge should be obtained with additional analysis, possibly, outsourced analysis. Regarding one of the previously top addressed Chinese zones of influence, Confucius Institutes, for example, there is an inconsequential registering of funds provided.

Given the diversity of the different topics which experts indicate as potential risks from cooperation with China, two were selected to illustrate the risk related to research cooperation: human bodies (bio) as well as hearts and minds (cognitive).

3.1.1.1. Biosecurity

In January 2024, the U.S. Congress introduced the BIOSECURE Act[114] which listed several official Chinese documents that upheld previous statements by U.S. intelligence accusing Beijing of gathering genetic information about U.S. citizens "in ways that could harm national security."[115] Since 2022 BGI, formerly known as Beijing Genomics Institute, is part of the Department of Defense's list of PRC Military Companies.[116] The Act also stated that BGI is engaged in a global campaign to collect foreign people's genetic data. Reacting to the Act, the representatives of the company said to GenomeWeb portal, "none of BGI is in any way controlled by or linked to the Chinese government or the military."[117] On 15 May 2024, the U.S. House Committee on Oversight and Accountability voted to advance the BIOSECURE Act, with amendments that "allow existing contracts with Chinese "companies of concern" to continue until 2032."[118]

---

[112] *Law on State Defense Service.* Likumi.lv. Last modified December 5, 2023. Retrieved on December 16, 2024 from https://likumi.lv/doc.php?id=107337&mode=KDOC.
[113] *Science Latvia.* Accessed December 25, 2024. https://sciencelatvia.gov.lv.
[114] U.S. House of Representatives. *BioSecure Act.* Select Committee on the CCP. Last modified December 2023. Retrieved on December 16, 2024 from https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/text-biosecure-act.pdf.
[115] *Congress Wants to Ban Chinese Genomics Firm BGI from U.S.* NBC News, July 12, 2023. Retrieved on December 16, 2024 from www.nbcnews.com/politics/national-security/congress-wants-ban-china-genomics-firm-bgi-from-us-rcna135698.
[116] According to several publications, in May 2024, it was going through rebranding to avoid sanctions.
[117] GenomeWeb. "Congress Introduces Bill to Prevent Medical Providers from Using BGI, MGI, and Affiliates' Products." *GenomeWeb*. Last modified January 26, 2024. Retrieved on December 16, 2024 from www.genomeweb.com/sequencing/congress-introduces-bill-prevent-medical-providers-using-bgi-mgi-and-affiliates-products.
[118] European Biotechnology. "Biosecure Act Could Affect Half of U.S. Biopharmaceutical Development." *European Biotechnology*. Last modified June 19, 2024. Retrieved on December 16, 2024 from https://european-biotechnology.com/latest-news/biosecure-act-could-affect-half-of-us-biopharmaceutical-development.

In 2019, the company mentioned in the BIOSECURE Act, BGI, as one of the world's largest genomics organizations opened its new facilities at Lidostas Parks, an area situated nearby Latvia's main airport[119]. The Investment and Development Agency of Latvia mentions this as an achievement; "a striking example of how the agency attracts foreign investment and successful companies to Latvia."[120] The article, titled "China Meets Europe in the Baltics", quoted the co-founder of BGI Dr W. Jian. He said, "Today, we sequence more DNA than any other organization around the world." He explained, "A couple of years ago we established our first European Genome Research Centre in Copenhagen[121] to accelerate innovations, genomics, and research and applications across Europe. In November 2019, MGI Tech Latvia, a subsidiary of BGI Group specializing in the development and manufacturing of gene-sequencing equipment, opened its first state-of-the-art production site in Europe. Our plans are to export gene sequencing equipment to the European Union, Africa, and the Middle East." That same day, MGI Tech Latvia launched the "10 Million Single-Cell Transcriptome Project (scT10M)" - a collaboration with scientists around the world "to sequence and analyze 10 million cells in an effort to build a comprehensive single-cell transcriptome map to be shared with the scientific community." [122]

A qualitative workforce, as mentioned by W. Jian, was among the priorities to select Latvia for opening a company " –We've already invested 15 million euros and are planning to recruit around 100 highly skilled professionals. In the first stage, we'll continue to promote the field of gene sequencing with our laboratory and production site here. In the next stage, we're planning to develop a technology center, which will help Latvia become one of the leaders in the life sciences in Europe. Everyone has probably heard in the news that BGI, the Wuhan National Bioindustry Base, and the Ministry of Economics of Latvia signed a Memorandum of Understanding at the annual 16+1 summit last year to build a Life Science and Technology Centre in Latvia. The center will serve as a platform for research and innovations in life sciences."

In 2019, MGI Tech Latvia already had active ties and cooperation with Latvian research institutions, for instance, with the Institute of Clinical and Preventive Medicine.[123] In the first days of BGI in Latvia, its co-founder said, "We're very serious about setting up research facilities and educational programs. For example, we've already put up a genetic sequencer at the House of Science of the University of Latvia."[124] Later on, multiple partnerships with MGI Tech Latvia were established; for

[119] In 2017, Latvia signed a Memorandum of Understanding with BGI.
[120] Labs of Latvia. "BGI China Meets Europe in the Baltics." *Labs of Latvia*. Last modified December 29, 2019. Retrieved on December 16, 2024 from https://labsoflatvia.com/en/news/bgi-china-meets-europe-in-the-baltics.
[121] The University of Copenhagen, Alma Mater of one of the BGI co-founders, (Yang Huanming), also get into the media agenda as the Chinese professor at the University of Copenhagen got under scrutiny due to undisclosed ties to the Chinese military. For more details see: BioSpace. "Danish University Researcher Under Scrutiny Due to Ties with Chinese Military Studies." *BioSpace*. Last modified November 19, 2021. Retrieved on December 16, 2024 from www.biospace.com/article/danish-university-researcher-under-scrutiny-due-to-ties-with-chinese-military-studies.
[122] MGI Tech. "MGI and European Partners Launch Project to Sequence and Analyze 10 Million Cells." *MGI Tech*. Last modified November 28, 2019. Retrieved on December 16, 2024 from https://en.mgitech.cn/news/108.
[123] University of Latvia. "HPylori Eradikācijas Shēmas Optimizācija Masveida Kunga Vēža Prevencijas Pasākumiem." *University of Latvia*. Last modified March 31, 2022. Retrieved on December 16, 2024 from www.lu.lv/zinatne/programmas-un-projekti/es-strukturfondi/eraf-sam-1111-praktiskas-ievirzes-petijumi-2karta/hpylori-eradikacijas-shemas-optimizacija-masveida-kunga-veza-prevencijas-pasakumiem.
[124] Labs of Latvia. "BGI China Meets Europe in the Baltics." *Labs of Latvia*. Last modified December 29, 2019. Retrieved on December 16, 2024 from https://labsoflatvia.com/en/news/bgi-china-meets-europe-in-the-baltics.

example, the first Latvian genome mapping.[125] BGI Research Foundation Latvia was registered in 2022.[126]

In September 2022, the Latvian Biomedical Research and Study Center became a co-host of the 17th Annual Meeting of the International Conference on Genomics, which was held in four Chinese cities with one special event in Riga (titled OMICS Advances in Africa and Europe).[127] According to the conference's website, BGI, BGI Research, MGI Tech Latvia and Latvian Biomedical Research and the Study Centre were all part of the organizing committee.

In May 2023, MGI Tech Latvia published the following update, "In a significant move that further solidifies its commitment to advancing life science technology, MGI Tech Co., Ltd. ("MGI") is proud to announce the launch of its overseas production line in Latvia. Under the subsidiary name Latvia MGI Tech[128], SIA ("MGI Latvia"). The company has established a large-scale facility in Riga to assemble and produce the state-of-the-art DNBSEQ-G400* gene sequencing instruments and HotMPS** reagents. This strategic expansion marks a significant milestone for MGI's growth in Europe, enabling the company to provide cutting-edge solutions for its customers and partners in the region."[129]

These and other MGI Tech Latvia related equipment are mentioned on the webpage of the University of Latvia Biomedicine Institute in the Section on the Genome Centre, which operates the Latvian National Biobank, including the EU program 1+ million genome.[130] The EU program 1+MG initiative aims "to enable secure access to genomics and the corresponding clinical data across Europe to support groundbreaking research and health policy making and incentivize personalized healthcare treatments with the potential to improve disease prevention".[131] The head of the institute, in the MGI Tech Latvia promotion video, talked about the benefits of long-term cooperation with MGI Tech Latvia, obtaining not only technologies, but also knowledge.[132] Also, cooperation regarding equipment sharing and research partnerships with other entities is listed on MGI Tech's web page.[133]

A disclaimer is written in the previously mentioned article highlighting technical support for major European universities and research institutions. The following information is mentioned: "Unless otherwise informed, all sequencers and sequencing reagents are not available in Germany, USA, Spain, UK, Hong Kong, Sweden and Belgium." Within the last few years, the U.S. National Counterintelligence and Security Centre issued multiple warnings, saying that China is investing in a

---

[125] University of Latvia. " Integrētas Latvijas populācijas genoma variāciju datubāzes izveidošana un tā pielietošana individualizēta metabolo slimību ģenētiskā riska noteikšanai." *University of Latvia*. Last modified November 30, 2023. Retrieved on December 16, 2024 from https://biomed.lu.lv/project/1-1-1-1-20-a-126/.

[126] The Register of Enterprises of Latvia. "Legal Entity Information." *Register of Enterprises of Latvia*. Last modified December 26, 2024. Retrieved on December 16, 2024 from www.ur.gov.lv/en/search-results/?search=40008316360.

[127] For instance, in the Science Latvia published report, information in the section on events doesn't reflect this event.

[128] The company can be found in annual self-reports of several Scientific Institutions in Latvia.

[129] MGI. *MGI Launches Overseas Production Line of DNBSEQ-G400 Sequencer in Latvia*. MGI Technologies, 2024. Retrieved on December 16, 2024 from https://mgi-tech.eu/en/news-events/mgi-launches-overseas-production-line-of-dnbseq-g-400-sequencer-in-latvia.

[130] University of Latvia. *Genome Centre Services*. Biomedicine Department, 2024. Retrieved on December 16, 2024 from https://biomed.lu.lv/pakalpojumi/servisa-centri/genoma-centrs-2.

[131] European Commission. *One Million Genomes Initiative*. Digital Strategy, 2024. Retrieved on December 16, 2024 from https://digital-strategy.ec.europa.eu/en/policies/1-million-genomes.

[132] YouTube. *[Video] – "Genomic Revolution: Impacts and Future"*. Retrieved on December 16, 2024 from www.youtube.com/watch?v=rJsVJe8vh70.

[133] University of Latvia. *Project Information: Genomics and Health*. Biomedicine, 2024. Retrieved on December 16, 2024 from https://biomed.lu.lv/project/1-1-1-1-20-a-126.

"biotech revolution".[134] Among other organizations, BGI is mentioned. BGI activities collecting samples were named as a threat to national security.[135]

In 2022, in an interview to the Washington Post, the representative of the Latvian counterintelligence entity, the Constitution Protection Bureau of Latvia (SAB), said, "The activity of Chinese companies in Latvia is associated with intelligence risks; therefore, such companies are under the attention of security services."[136] The same approach was confirmed in the interview in 2024.

In May 2024, Aarhus University decided to end its collaboration with Chinese genomics research companies "owing to what the university describes as 'a change in the security landscape' and 'the fear that data will be misused for unethical purposes'."[137] In June, the University of Copenhagen took a similar decision, as did the Technical University of Denmark. The Vice-Dean of this university, R. Larsen said that the reason was the possible (risk of) "inappropriate knowledge transfer."[138] In July 2024, as indicated by a representative of HEI A, an unwritten decision not to use Chinese equipment was introduced at the university.[139]

This and other recent decisions on foreign cooperation with non-democratic countries, indicates formal and informal information flows on security topics that reach scientific institutions. Besides the security services, which mentioned for the first time possible risks to academic cooperation with China, there is another actor promising to take a leading role in raising awareness of academic personnel.

According to multiple sources, in June 2024, the Latvian Ministry of Foreign Affairs took the leading role in raising awareness for possible foreign interference and the importance of research integrity. A meeting was held with the participation of Ministries, including the Ministry of Education and Science, scientific institutions and the security services, who voiced potential risks and concerns about cooperating with foreign research centers and universities. Prior to this meeting, as shared by several interviewed leaders of the Latvian HEIs, there were no such type of joint forums to discuss research integrity from the perspective of national security from any other governmental institution in Latvia. This constitutes a unique Latvian practice, as it could potentially cover the main identified gap of legitimization of mitigation.

A few weeks prior to the aforementioned meeting, a representative of HEI B, indicated that while lacking state-level guidance on potential risks and threat mitigation, universities are under pressure to be more active internationally, also - to compete in university ratings. However, he recalled a couple of seminars on research security.

---

[134] National Counterintelligence and Security Center (NCSC). *China and Genomics: A Fact Sheet*. U.S. Department of Homeland Security, 2021. Retrieved on December 16, 2024 from www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

[135] ICG17 Riga. *International Conference on Genomic Research*. International Conference Group, 2024. Retrieved on December 16, 2024 from https://icg17riga.com.

[136] The Washington Post. *China's DNA Sequencing Push: A Global Health and Security Threat*. The Washington Post, 2023. Retrieved on December 16, 2024 from www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid.

[137] Aarhus University. *Top Researcher in Genomics Leaves After University's Decision to End Chinese Collaborations*. 2024. Retrieved on December 16, 2024 from https://omnibus.au.dk/en/archive/show/artikel/topforsker-inden-for-genomforskning-siger-op-paa-au-efter-universitetets-beslutning-om-at-stoppe-kinesiske-samarbejder-1.

[138] ScandAsia. *Danish Universities Break Away From Chinese Partners*. ScandAsia News, 2024. Retrieved on December 16, 2024 from https://scandasia.com/danish-universities-break-away-from-the-chinese-partners.

[139] In-depth interview conducted July 2024.

As outsourced seminars (by the security services) are mainly to leadership, it is also important to keep in mind changes of personnel and the need to routinely update the risks. This creates an additional need for a holistic and comprehensive approach, also reflecting on European, national and regional risks and practices for mitigation. The representative confirmed that recent experience with limiting cooperation with Russia on one hand helped to prioritize security. On the other hand, since there is no clear guidance on China, interaction with Chinese students, researchers and institutions is not perceived with the same sense of urgency. According to the representative, also in early 2024, the HEI B had a seminar with invited outside experts on security (representing the security services) to receive updates on risks to national security in academia and research. The HEI B is working on a way to transmit this knowledge to personnel but has not implemented a system yet.

In general, as could be observed through the conducted interviews with leaders and scientists, awareness of potential foreign interference in the field of academia and research increased due to Russia's full-scale invasion of Ukraine. Written guidance on further cooperation with the aggressor-state resulted in additional focus on other non-democratic actors, including those aligned with Russia, possibly benefiting Russia. However, while there is a clear vision of non-relation with Russia, it is foggy when it comes to relations with other non-democratic counties. On one hand, universities are interested in international collaboration, as international cooperation is among the main priorities in science, technology and innovations, as indicated in guidelines for 2021-27[140] - promoting its universities, welcoming new students, engaging in research, and bringing finances to mitigate financial risks. On the other hand - knowledge security is getting on the agenda, also through regional cases of espionage or EU level initiatives.

Additionally, the Latvian Ministry of Foreign Affairs is committed to continue these meetings, to provide updates on knowledge security and research integrity. With this, the Ministry of Foreign Affairs could fill in the gap of the missing coordination body, one of the main problems mentioned by interviewed respondents, responsible for research integrity at their universities. For instance, several non-systematic interactions with security services, mainly on an individual (single university) basis, were mentioned by universities in the search for more clarity on threats and risks incoming from foreign nations.

However, establishing the cooperation space for leadership, and making it horizontal, including several universities, does not ensure that necessary further communication and data exchange within the organizations will take place. There is a clear need, from the interviewed representatives of leadership, as well as researchers, to establish ways to prioritize national security while maintaining the freedom of research and making it a routine. Regarding interviews, the sensitivity and in-depthness of the topic did not allow the professional managers to feel comfortable discussing national security issues. Focal security point might be a part of the solution when it comes to the informed decision-making process.

Another practice to consider, especially for regional institutions, was indicated in an interview with a representative of a HEI C. In the interview the representative said that from time to time, the university invites local focal points from the Latvian State Security Service. These practices allow them to keep the institution up-to-date, as well as to establish mechanisms for whistleblowing - an important component in risk mitigation. According to the representative, when the Latvian government strategy was to increase cooperation with China, he also tried to increase cooperation; however, the interest from Chinese diplomats arose only when the university considered to start a new program on cyber direction. At that time, the level of potential risks from cooperation was evaluated as high and

[140] Ministry of Education and Science of Latvia. *Academic Censorship Concerns in Latvian Universities*. 2024. Retrieved on December 16, 2024 from www.izm.gov.lv/lv/media/11501/download?attachment.

cooperation did not happen. To prove this, he said that Chinese language classes supported by the Chinese government (with the teacher who previously utilized the university facilities) also are not available anymore.

In summary, academic leadership would benefit from targeted activities to increase their confidence and awareness of potential risks while collaborating with foreign counterparts. Also, it is essential to ensure exchanging best practices, including general awareness on changes in the security landscape with the focus on research and academia. The last, for example, would widen threats from fundamental and applied research to the cognitive domain, including social sciences and knowledge related not only to the body of humans, but also their minds. The relevance of cognitive domain in national security has been already addressed in this report. The next section provides some examples of discourse power based on technologies and social sciences, frequently overlooked by the security researchers.

3.1.2. Emerging risk in the cognitive domain – a discourse superpower

According to a researcher C. Singleton, China is aiming to become a discourse superpower "to advance its hegemonic ambitions."[141] In "Cognitive Combat: China, Russia, and Iran's Information War Against Americans" he wrote, "Distinct from soft power, "discourse power" seeks to set and shape global narratives to bolster China's composite national strength and international influence."[142] Shaping its influence in different environments, the academic environment remains crucial.

In May 2024, the annual 6th conference of the Baltic Alliance for Asian Studies, an alliance of five Baltic universities (Tallinn University, University of Latvia, University of Tartu, Vilnius University and Vytautas Magnus University) was organized by the University of Latvia. Prior to the conference, the Centre for Asian Studies at the Vytautas Magnus University, one of the alliance members, made a statement.[143] In this statement, the Centre informed the public about its decision to withdraw from the "Dialogue of Asian Civilizations in Accelerated Globalization" conference. The decision was explained as follows, "We uphold the unified stance of the Baltic Alliance for Asian Studies institutions which was prompted by the opaqueness of the decision-making of the conference and the biassed outcomes. The Centre for Asian Studies strongly supports the principles of academic freedom, impartiality, and open discussion, which, regrettably, were not followed by the organizers of the aforementioned conference. As a result, all six participants affiliated with Vytautas Magnus University expressed their will to be removed from the conference program."[144]

On the same day, Vilnius University made a similar statement, saying that the Institute of Asian and Transcultural Studies at Vilnius University had withdrawn from the conference. Their statement said, "This decision was prompted by the conference organizers 'attempts at academic censorship and their pro-Chinese government stance."[145] Both Lithuanian universities also requested not to use the Baltic

---

[141] Bowman, B. (Ed.). *Cognitive Combat: China, Russia, and Iran's Information War Against Americans*. Foundation for Defense of Democracies, 2024. Retrieved on December 16, 2024 from www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf.

[142] *Ibid*

[143] Centre for Asian Studies, Vytautas Magnus University. *Statement Regarding the Conference on Dialogue of Asian Civilizations in Accelerated Globalization*. 2024. Retrieved on December 16, 2024 from https://asc.vdu.lt/2024/05/centre-for-asian-studies-statement-regarding-the-conference-dialogue-of-asian-civilizations-in-accelerated-globalization.

[144] *Ibid.*

[145] Faculty of Social Sciences, Vilnius University. *Asia and Transcultural Studies Institute Events*. 2024. Retrieved on December 16, 2024 from www.fsf.vu.lt/azijos-ir-transkulturini-studij-institutas/instituto-ivykiai-2.

Alliance for Asian Studies name in association with this conference. More details came up in the LSM report, where a representative of the Vilnius University called the cases of taking off China-sensitive references from the conference "the first known" case of censorship in the Baltics. A researcher K. Andrijauskas, representative of the University, said to LSM, "we have received news that the Estonian papers have also been withdrawn. What do all these papers have in common? They are on subjects that are considered sensitive for Beijing - Taiwan, Hong Kong, the historical repression of the Chinese Communist Party. These are the topics that have been removed. This is the first case of academic censorship in the Baltic states that I know of."[146] In an interview with Latvian Television, Guntars Kitenbergs, the Prorector of the University of Latvia, said it was a misunderstanding and that the papers had been restored in the program of the conference.[147]

Five years ago, the investigative media Re:Baltica in its article on China, quoted a former rector of the University of Latvia, Mārcis Auziņš, who described his dinners at the Chinese ambassador's residence. The article said, "Dinners at the Chinese ambassador's residence were a part of a regular working relationship for the former rector of the University of Latvia, Mārcis Auziņš. Sometimes at those dinners he would receive hints about the university's work. "You know, Rector, a lecturer such and such cooperates with [Taiwan's] mission (..) You know that our government supports you, my government may not like it," Auziņš recounts one of the conversations. The wider public does not know that China generously supports its Confucius Institutes."

In July 2024, 187 Confucius Institutes operated in 41 European countries, and 348 Confucius Classrooms were also established in 31 countries.[148] Both operate in Latvia. In April 2024, Latvian Confucius Institute was awarded in a globally competing 300 Confucius Institutes "Outstanding Communication Confucius Institute of 2023."[149] As of Summer 2024, the Confucius institute is still active at the University of Latvia, networking not only with Latvian secondary schools (Chinese language classes) and HEIs in Latvia visiting and collaborating with regional universities, and also with the Confucius Institute in Estonia – on the Baltic level.

The Confucius Institute, as could be followed by publicly available information in the social media of the involved institutions and persons, also plays a crucial role in connecting with regional institutions. There might be different combinations of approaches – solo visits of representatives of the Confucius Institute, as well as accompanied by Chinese diplomats, and solo visits of Chinese diplomats – formal and informal visits, coming to meet universities' leadership and staff, as well as visiting campuses and dorms.

According to the Congressional Research Service, some Members of Congress considered that the Confucius Institutes were used to recruit "influence agents".[150] The report said, "according to some experts, the activities of Confucius Institutes are narrow in scope, and they have an incentive to avoid controversial activities, such as disseminating PRC propaganda, on the one hand, and broaching topics that are politically sensitive in China, on the other. Some academic observers counter that Confucius

---

[146] LSM.lv. *Concerns Over Academic Censorship: Latvian Universities Withdraw from Asian Studies Conference.* 2024. Retrieved on December 16, 2024 from www.lsm.lv/raksts/zinas/latvija/17.05.2024-bazas-par-akademisko-cenzuru-augstskolas-atsaka-dalibu-azijas-studiju-konference-latvijas-universitate.a554477.

[147] LTV ziņas. *Akadēmiskā cenzūra vai pārpratums?* LSM. May 17, 2024. Retrieved on December 16, 2024. https://replay.lsm.lv/lv/skaties/ieraksts/ltv/327531/akademiska-cenzura-vai-parpratums.

[148] China International Education Foundation (CIEF). *Confucius Institutes in Europe and Their Impact on Education.* 2024. Retrieved on December 16, 2024 from www.cief.org.cn/qq.

[149] 拉脱维亚大学孔子学院 Confucius Institute at University of Latvia. *Official Website.* University of Latvia, 2024.

[150] Congressional Research Service. *China's Espionage Threats and U.S. Research Security.* Report IF11180, 2024. Retrieved on December 16, 2024 from https://crsreports.congress.gov/product/pdf/IF/IF11180.

Institutes exert influence in U.S. universities through PRC board members 'interpersonal relations and the Institutes 'involvement in China-related programs and connections to educational and research opportunities in China."[151]

Confucius Institutes are sharing narratives that support the Chinese government. According to a report on Chinese influence operations, "several universities have also decided to shut down the Confucius Institutes they hosted, invoking, in particular, an infringement of academic freedom."[152] Among the risks are mentioned teachers, learning materials, financial influence, self-censorship, effects on non-Confucius Institute affiliated teaching staff, effects on other researchers and espionage.

Regarding the U.S., almost all Confucius Institutes have been closed recently, "section 1062 of the National Defense Authorization Act for Fiscal Year 2021 and Section 10339A of the CHIPS and Science Act of 2022 restricts DOD and NSF funds to institutions that host a Confucius Institute. Additionally, Sections 1044 and 1045 of the National Defense Authorization Act for Fiscal Year 2024 made modifications to the definition of a Confucius Institute and terminated DOD's authority to issue a waiver to institutions who maintain a Confucius Institute."[153] The Congress report said that from 118 Confucius Institutes at the peak in 2018, only seven remain as of 2022.[154]

Also in Europe, the number of the Confucius Institutes was reduced. Some, such as the Free University of Brussels, did it to reflect security-related issues - "the institute's director was accused of spying for Beijing. Belgium also expelled a Chinese doctoral student in 2021 because his academic work was a cover for his intelligence work, according to Belgian media."[155]

There is a risk of rebranding the Confucius Institute, as indicated by The Diplomat, in order to cover its operations.[156]

3.1.3. Conclusions for Latvia

The Latvian academic community, as reflected on different levels, took measures to end cooperation with the Russian Federation, reacting to the full-scale invasion in February 2022. As illustrated by an interviewed representative – this decision was quick, undebatable and, on a personal level, for some, even painful. Contacts with Russia, prior 2022, were identified as significantly more intense than relations with China. Moreover, involvement of academics in international projects was based also on historical ties and years of personal, rather than institutional, cooperation. As described by one interviewed representative of academia, it was a matter of language, cheap (regarding travel and accommodation costs) international conferences and long years of ties of cooperation, also including publications. Mentioned factors (cooperation, conferences, publications) hold significant relevance for a specific rating of universities. To ensure further commitment regarding other countries and risks, clear communication from the responsible institutions is needed. Also, a representative of SAB

[151] *Ibid.*
[152] Charon, P., & Jeangene Vilmer, J.-B. *Chinese Influence Operations: A Machiavellian Moment*. Institute for Strategic Research, Paris, 2021.
[153] American University. *Actions Taken in Response to Research Security Concerns*. Association of American Universities, 2024. Retrieved on December 16, 2024 from www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Actions-Taken-Research-Security.pdf
[154] Congressional Research Service. *China's Espionage Threats and U.S. Research Security*. Report IF11180, 2024. Retrieved on December 16, 2024 from https://crsreports.congress.gov/product/pdf/IF/IF11180.
[155] Politico. *EU's Espionage Problem: Why It's So Difficult to Catch Spies*. Politico, 2024. Retrieved on December 16, 2024 from www.politico.eu/article/eu-spy-problem-heres-why-its-so-difficult-to-catch-them-espionage-russia-china.
[156] The Diplomat. *The Rise and Fall of Confucius Institutes in the U.S*. The Diplomat, November 2023. Retrieved on December 16, 2024 from https://thediplomat.com/2023/11/the-rise-and-fall-of-confucius-institutes-in-the-us.

indicated that risks remain from Russia, referring to collaboration with researchers from Russia via other countries and non-Latvia based institutions.

The security services communication tradition in Latvia could be described as maintaining a low profile with annual reports and very rare public comments to the media. Further, the awareness about potential risks from China contrasts with strategic narratives promoted by the Latvian government for a decade to increase cooperation, supported on a cross-institutional level, including the Ministry of Foreign Affairs, the Ministry of Economy (with the special role of the Investment and Development Agency of Latvia), etc. The reflection of changes in the security landscape could not be ignored by those who previously promoted cooperation.

While the security services, in the case of Latvia - Military Intelligence, State Security Service and the Constitution Protection Bureau - cover specific angles of national security, there might be additional levels of control, to protect data relevant to national security. In the case of the U.S., the DoD has a set of specific requirements for those projects supported by governmental funding and it serves as an additional layer of control, where the academic institutions are responsible for data gathering and submitting. As indicated by a representative from the Ministry of Defense, it is Military Intelligence who is doing research on potential cooperation, not the academic entity itself. Most probably the system remains the same, without asking universities and research centers to be more active in self-assessment. At the same time, it is crucial for universities and research institutions to outsource needed knowledge gathering regarding potential cooperation.

The representatives should have different ways (formal and informal) to address professionals for due diligence on the phase of negotiations, after preliminary internal analysis of potential cooperation.

The Emerging Triangle of the Ministry of Affairs (and other Ministries), Security Services and academia, if not lacking commitment, would be an important component to strengthening national security in the field of research security. Also, as mentioned by the security experts, it is relevant that the Ministry of Foreign Affairs is responsible for Goods Export Control. However, besides communication with the leadership, it is essential to ensure that there is vertical communication with the research and academic institutions, to affirm that security culture is part of everyday activities.

The Latvian Science Council, the main body covering foreign cooperation with universities, including Horizon, demonstrated an increased level of awareness, referring mainly to cooperation with the Ministry of Interior on providing a legal basis for entering the country. The academic sector would benefit from templates, best practices, marking it as the most important parts of research security workshops. At the same time, as pointed out by an interviewed representative of the Council, in cooperation with other European and non-European countries, observed a less security-oriented agenda, more "relaxed" attitude, compared to local higher educational institutions and research centers.

Academia-related respondents did not consider the Ministry of Education and Science as a potential leader in the field of knowledge security, pointing to national security entities. Given the fact that higher education institutions and centers could be connected to other ministries, it makes coordination even more complicated. Regarding national security services in Latvia, they keep a low-level public profile, mainly focusing on annual actualization of threat. Academic security engagements, as noted by representatives of academia and representative of security services, were unsystematic.

3.2. Case of Estonia

The following chapters provide a brief overview of the key issues related to research security in Estonia, as described by the interviewees from different backgrounds and organizations. The opinions and views expressed have been generalized and structured with the aim of finding a meaningful compromise between the weight of past experiences and the pull of future developments in order to improve the state of research security in the country.

3.2.1. A learning curve: gaps and concerns

The topic of research security has recently emerged as a significant concern on the academic policy agenda in Estonia. The Estonian respondents identified the need to establish a clear definition of research security, delineating its scope and exclusions in relation to other related concepts, such as knowledge security, research integrity, information security, protection of intellectual property, and operational security in academia. All respondents concurred that it is of paramount importance to ensure that all national stakeholders (including individual researchers and academic staff, security experts, universities and research and development institutions, government officials, politicians) have a common understanding of the term and, ideally, a nationally agreed and confirmed version of the definition that also reflects the positions of the European Union regulatory bodies and research institutions.

Russia's unprovoked aggression against Ukraine has significantly influenced perceptions regarding the moral implications of international research collaboration with authoritarian regimes while the legal sanctions and other restrictions have effectively impeded any rational institutional cooperation with Russian and Belarusian entities. In contrast to the situation with Russia and Belarus, navigating the complexities of Chinese influence in academia is more challenging, particularly in the absence of clear guidelines or principles on research security. A general official memorandum of academic and research cooperation exists between Estonia and China. However, it does not regulate any particular area, nor obligate anyone to undertake any specific projects or programs. Moreover, Chinese influence activities in academic institutions are often perceived as opaque and subtle, with few apparent restrictions, minimal red zones, and a multitude of attractive offers or even useful opportunities for research and innovation aimed at addressing global challenges and technological advancement in emerging areas of science. As the national legislation does not explicitly delineate the boundaries of academic freedom nor provide risk-benefit assessment solutions, research policy makers in Estonia and the leadership of academic institutions must rely on their own professional judgement and the support of security authorities (e.g., Estonian Internal Security Service (KAPO)).

There is limited human capacity within government bodies to cover all the complexities associated with research security issues, as there is neither a dedicated policy area nor a separate department established to maintain and analyze situational awareness, accumulate relevant expertise and disseminate the know-how. In other words, there is no single point of responsibility within the government structures when it comes to coordinating a comprehensive approach to ensuring research security in Estonia. Some of the most important actors in this area are the Ministry of the Interior, the KAPO and the Estonian Police and Border Guard Board, whose tasks include, among others, background checks of foreign non-EU students and migrant workers, countering espionage and foreign influence activities. As some recent cases have shown, the concerns of Estonian academia have gradually become part of the working agenda of internal security, although its officials mostly view the issue through the prism of threats to national security (which is their mandate), and the so-

called grey (undiscovered) zones of research security may remain overlooked due to the limited capacity of scientific focus within the internal security apparatus.

Civil ministries and their agencies responsible for research, development, and innovation, on the other hand, are more exposed to and experienced in the peculiarities of scientific and applied research, and their officials are more knowledgeable about data protection and intellectual property rights, but they may lack the deep understanding of evolving security threats and toolbox of malicious influence activities related to the rapidly changing geopolitical situation. As internationalization and attracting new grants and foreign investments are among the most important general drivers for research and innovation, security concerns are still seen as more specific cases to be dealt with primarily by security authorities.

The current state of research security in Estonia is largely unmapped, resulting in a lack of comprehensive knowledge at various levels of policymaking. A majority of national politicians have a general understanding of geopolitical threats but have not yet formulated a clear political appetite for regulating research security issues in Estonia. On the strategic level, cooperation with China is a legitimate activity, although it is not entirely free of security concerns. At the operational level, there is a general perception that some guidelines on research security can be established. However, it is understood that their implementation will remain voluntary for academia. At the tactical level, each HEI, research entity, or even individual researcher relies on their threat awareness, previous experiences, and institutional support, if available, internally or externally (e.g., KAPO). At present, the state assumes that universities and other research entities have their own security measures in place. However, in the absence of clear official requirements for research security, there is no formal procedure nor established competence to assess their compliance.

According to the interviewed respondents, a lack of systematic approach to risk-based analysis in research security in Estonia is evident. While the general awareness of academia on threats to research security in Estonia is difficult to assess, it seems that the situation is improving, at least in part, due to increased vigilance. This is largely attributed to the publicity surrounding Russian and Chinese recruited spies in Estonian universities and the training provided by KAPO to academic personnel and researchers over the past few years. Nevertheless, it would be erroneous to assume that the aforementioned measures have been implemented in their entirety across all research institutions and their employees in Estonia.

The recent cases of the arrest and conviction of university researchers for espionage against Estonia have caused considerable shock and disquiet within the academic community. Many colleagues have described the individuals in question as trusted professionals and honored peers. These cases have served to reaffirm the view that HEIs are not immune from the activities of foreign intelligence agencies. Tarmo Kõuts, a marine scientist at the time of the case at the Tallinn University of Technology, was convicted by the Estonian authorities in 2021 for spying against Estonia on behalf of China. As confirmed by KAPO, Kõuts was recruited in 2018 on Chinese territory by China's Intelligence Bureau of the Joint Staff Department of the Central Military Commission.[157]

A further case from the Estonian academic community has demonstrated that the fields of social research and humanities, in addition to those of hard science and technology, may be regarded by foreign intelligence services as offering potential for espionage activities. In June 2024, Viacheslav Morozov, a former professor of political theory at the University of Tartu, was found guilty of activities against Estonia. He had been conveying information about Estonia's internal, defense and

[157] ERR News. *Estonian Marine Scientist Sentenced for Spying for China*. ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1608148489/court-sentences-estonian-marine-scientist-to-prison-for-spying-for-china.

security policies, its critical infrastructure, political situation, allied relations, integration, and social cohesion to the foreign military intelligence agency of the General Staff of the Armed Forces of the Russian Federation. As stated by KAPO, Morozov was recruited while he was a student at St. Petersburg State University in the 1990s and underwent training at a military faculty in Russia.[158]

While evidence-based espionage activities are addressed practically by counterintelligence and legally by the legal system, other influence and interference actions within academia may be of an obscure nature and therefore fly under the radar of security services, not to mention the leadership or management of HEIs, who may not be equipped to identify some specific threats or mutating risks. Furthermore, respondents from HEIs acknowledged that the awareness of researchers and academic staff about geopolitical threats and related risks (including malicious foreign interference and influence operations) has gradually increased in recent years, as public and political pressure to safeguard international academic cooperation in the context of national security responsibilities has increased. In other words, there have been several strong signals highlighting the evidence of a changing environment and increasing confrontation, so that the academic community cannot completely distance itself from security issues.

Nevertheless, as expressed by several interviewed respondents, at the moment, it seems unwise and impractical for Estonian universities to eliminate or scrutinize academic and research cooperation just because it might have a Chinese element. A proper framework and policy guidelines are needed on whether and how to consider research security issues when dealing with multi-party projects and programs involving Chinese or China-friendly entities. Since there is very limited competence within universities and research organizations to assess the variety of risks and threats associated with foreign malign influence, internal procedures cannot be haphazard and must follow a systematic approach to help the academic community to understand the steps for flagging an issue of concern and the follow-up actions needed to mitigate the risks.

The extent of research cooperation on the individual level remains largely unidentified, as there are currently no resources or established practices to monitor peer-to-peer academic engagements. This includes activities such as co-supervision of theses, co-authorship of articles, journal reviewers, summer schools, and personal travel grants, and other activities. In the event that some degree of skepticism exists towards questionable activities, there are no established regulations regarding the appropriate response to specific cases within academic or research organizations in Estonia.

Estonian universities and research institutions view the national security services as the primary reference point for research security issues. However, they are aware of the limitations of the relevant agencies, particularly in matters pertaining to the specific characteristics of scientific data, methodologies, and other non-security topics. All of the interviewed representatives expressed appreciation for the security trainings organized by KAPO for HEI leadership and management staff, as well as researchers. However, they noted that the attendance remains voluntary, and the number of participants is relatively modest. Moreover, a general attitude among researchers is that without a proper legal mandate, qualifications, procedures, and regulations, any university cannot be responsible for co-ensuring national security interests, especially in the context of a vague foreign influence in research and academic matters. Another point worthy of discussion is the potential impact of introducing a research security framework on academic freedom and international research projects. It is also important to consider the rational and reasonable range of sanctions that could be applied (if any) to national researchers or academic staff who make mistakes in research security matters.

[158] ERR News. *University Professor Found Guilty of Espionage Against Estonian State*. ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1609374515/university-professor-found-guilty-of-espionage-against-estonian-state.

Researchers and academic staff should understand the full range of malicious influence activities and their consequences, including financial dependency, data leakage, risk of blackmail, peer pressure, reputational damage, or self-censorship.

In 2020, the University of Tartu faced challenges in its public communication efforts when it applied censorship to certain critical China-related articles and social media posts due to its cooperation agreement with Huawei. This incident served as a valuable learning experience for the academic community in Estonia.[159] Nevertheless, in the absence of actuated cases, the issues of research security are consigned to oblivion. It is logical to allocate resources to the implementation of preventative measures which include roundtable discussions, training programs and crisis exercises.

In addition, given the sensitive nature of research security and the concomitant issue of academic freedom, it is unsurprising that many researchers and HEI managers perceive it as a challenging endeavor to guarantee an adequate level of safety and security while simultaneously avoiding the over-regulation of their routine. Furthermore, the tragic history of the Soviet occupation in Estonia serves as a reminder of the adverse consequences of science securitization, which was a standard practice in the totalitarian regime of the Soviet Union. As previously stated during the in-depth interviews with representatives of HEIs, academics in Estonia place a high value on transparency and independence in their research activities. Consequently, they would prefer to see less interference from regulatory bodies. However, when it comes to matters of national security, they are willing to cooperate with state authorities and security services, adhering to their guidelines and recommendations. One key outstanding question is who should bear ultimate responsibility for establishing standards, enforcing rules, and making judgments regarding research security.

As mentioned several times in the interviews, one of the main risks that could expose Estonian academia to foreign, and especially Chinese, influence is the unfortunate combination and confluence of several factors, such as low awareness about potential threats, limited financial and human resources, as well as chronic underinvestment in some areas. In this context, government cuts in research and higher education budgets intensify competition for available resources, not only nationally but also internationally, as the range of possible donors and partners expands. When national and EU research funding is constrained, Chinese (or China-related or influenced) sources may become more attractive to some researchers, HEIs and other research institutions because of their relatively greater accessibility and availability, as well as lower accountability. Moreover, as mentioned by several interviewees from HEIs, academic cooperation with China was verbally promoted by some external researchers through visiting scholars from other EU countries and was generally perceived as a positive sign based on previous successful experiences.

Representatives of Estonian HEIs have emphasized the importance of avoiding additional administrative burdens when designing recommendations on research security. They have noted that the limitation of resources is a very serious and ongoing challenge to all universities and research institutions in Estonia. The preference is to make a better use of existing structures and data collection methods to promote research security and monitor the situation. Moreover, they underscored the necessity of enabling open discourse on security matters and related risks in research, while maintaining a balance between these concerns and the tenets of academic freedom and information sharing traditions.

---

[159] ERR News. *Tartu University Removes China-Critical Social Media Post*. ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1110733/tartu-university-pulls-china-critical-social-media-post.
ERR News. *Paper: University of Tartu Refused to Publish Article on Huawei.* ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1056839/paper-university-of-tartu-refused-to-publish-article-on-huawei.

3.2.2. A way forward: vigilance and adaptation

The respondents indicated that Estonian academia could benefit from learning about research security fundamentals and adopting some useful practices from European and U.S. institutions, with due consideration for their applicability in the local context. While the EU endeavors to standardize the primary principles and universal approaches to research security at the European level, the representatives of Estonian academia express concerns about the division of tasks between universities and research institutions, grand agencies and foundations, and government authorities and security services (e.g. KAPO).

Given the distinctive characteristics of HEIs and research entities, as well as the experience of collaboration with China and the extent of Chinese influence activities within the country, the interviewed representatives of Estonian academia find it challenging to follow a set of general European rules in an effective manner. Instead, they advocate for a flexible national framework that considers the limited resources available within HEIs and research institutions to introduce new, significant tasks. For instance, as it was observed during the interviews, Estonian HEIs do not have a systematic approach to providing safety and security briefings to researchers or academic staff prior to their foreign work-related travels, even to countries such as China or other countries with which China has friendly relations. This is largely due to the assumption that the responsibility for conducting a travel risk assessment lies with the individual.

The current limitations of HEI leadership and management in creating or applying tools to pressure academic staff to abide by the principles of research security are a consequence of the absence of agreed policies or regulations. Those departments and researchers who work with classified materials or information adhere to the law on state secret protection, having passed security vetting by KAPO and obtained a personnel or institutional security clearance. This represents a very small group of researchers and teaching staff, whereas the majority of personnel have no systematic guidelines to follow. As some Estonian universities have ongoing cooperation projects with Chinese institutions, the state authorities (i.e. KAPO) are aware of them and key academic personnel have been trained to identify major risks of malicious influence and interference. In addition, these universities follow one of the main principles of cooperation - the nature of mutually beneficial outcomes - and approach the proposal on a case-by-case basis. The unilateral expression of strong interest in specific proposals gives rise to suspicions, as has occurred on previous occasions. For example, Chinese entities have previously suggested joint research projects to Estonian universities in the fields of information technologies and digital governance.

As research policymakers acknowledge and respect universities 'autonomy, they do not perceive any possibility of interfering in the internal affairs of higher education institutions, even in the event of evidence of a functionality gap related to research security issues. The state authorities, in particular the KAPO, provide training on the basics of counterintelligence as well as offer some useful advice on specific cases if consulted. However, it is clear that the core of research security lies within the universities and research enterprises. Delegating the responsibility to academia would result in an increased administrative burden, necessitating the identification of a solution to provide additional resources to HEIs and research entities for the establishment of a robust system of research security. This system would require the training of personnel, the management of know-how, the provision of training, and the implementation of procedures, among other measures.

The academic community in Estonia concurs with the view of research policymakers that enhancing research security must be achieved through a reasonable balance between openness and inclusiveness, as these are essential for the creativity, innovation, and progressive development of science and

technology, which is necessary to solve global problems in health, climate, economy, and other areas. The general understanding of potential risks supports the introduction of safety measures to prevent the misuse of research results, particularly when national security, human rights, and other sensitive topics are concerned.

In the view of the respondents interviewed, the visible activity of Chinese diplomats towards Estonian academia has been on the wane in recent years, as they may have come to recognize the limitations and ineffectiveness of such contacts. Nevertheless, China's state support to the Confucius Institute persists, as do some direct contacts between Chinese and Estonian HEIs and research entities. This calls for greater vigilance on the part of the relevant parties in Estonia at institutional and individual levels.

The respondents interviewed indicated that Estonia is not currently contemplating the establishment of a national research security officer office. However, they suggested that a job position with some corresponding responsibilities could be created within universities and research institutions if they deem the issue to be crucial for their operational functionality and to prevent any collateral reputational damage resulting from undermining national security concerns. In light of the dynamic shifts occurring in the global geopolitical and socioeconomic arenas, a significant change of mindset is required not only at the level of strategic or operational policymaking in research and higher education in Estonia, but also at the individual level of researchers and academic staff. This is necessary in order to minimize the impact of naivety and other human factors when it comes to international cooperation with China and other China-friendly countries (e.g., Central Asia, some Arab, African and South American states). Furthermore, academic collaboration with India, Brazil and Mexico appears to offer promising opportunities, although it may also entail certain potential challenges and security risks. Previously established guidelines and regulations pertaining to research integrity, data protection, and related matters must be revised and updated to account for evolving challenges to research security, with particular attention to dual-use technologies and research value chains where business interests may outweigh ethical considerations or security threats. This is particularly relevant in the context of various types of knowledge transfer, exchange programs, and international cooperation platforms.

Given the small size of Estonian academia, the inclusion of foreign scholarships and grants, foreign students and foreign researchers is considered one of the priority areas, as it can accelerate the attraction of new talent and/or funding, which consequently plays a crucial role in ensuring the sustainability of higher education and research institutions in Estonia. For human resources, separate programs are established for EU and non-EU nationals, with the latter showing more interest in and availability to study or work in Estonia, but at the same time may pose greater research security risks if there is any degree of Chinese influence. To mitigate the associated risks, several interviewees cited the Swedish and Australian experience as a good example of guidelines for enhancing security in academia.

The specific area of dual-use research and technologies was mentioned by both research policy-makers and representatives of HEI as an area that can serve as a good reference for working regulations and arrangements with clearly defined procedures, roles of stakeholders and responsible actors (including academia, research companies and public authorities), as well as a high level of harmonization between EU and national legislation.

Furthermore, Estonian policymakers consider it crucial to take into account the needs and specific circumstances of Estonian researchers when designing recommendations on research security. The success of their implementation will depend on the practical relevance to the daily work and operational environment of researchers and academic staff at HEIs. Estonian research policymakers

have observed that recommendations on research security cannot be merely a formal framework; rather, they must be a practical tool with clear guidance that can be easily understood and implemented. Involving researchers and academic staff of HEIs will ensure the sustainability of research security recommendations and may have a positive impact on the Estonian research system as a whole, as the adoption of the policy will be genuinely practical and not just a compulsory formality. Furthermore, the recent data breach at an Estonian R&D company[160], which was the victim of a cyberattack by a criminal gang led by a Russian national[161], emphasizes the necessity for a heightened focus on the safeguarding of large databases. This necessitates a specialized approach to ensure the primary tenets of information security (confidentiality, integrity, availability, and accountability).

Estonian government agencies should direct and assist the building of capacity within research organizations and HEI to assess security risks and their impact on research activities, including international cooperation with non-partners. The view of Estonian research policymakers is based on the shared understanding that academic institutions as organizations and researchers as individuals should have a habitual practice of maintaining adequate situational awareness and be competent to provide an initial threat assessment in order to be able to advise stakeholders on research security as appropriate.

In light of the potential time frame for the development of a comprehensive national framework, a network-based model of research security officers in HEIs and research entities could prove an effective interim measure for mitigating the risks associated with foreign interference (e.g. China-related) in Estonia's academic sector. The Estonian Research Agency could potentially provide support and coordination for the network platform, conducting respective training activities in collaboration with KAPO and other relevant authorities. Additionally, the Estonian Research Agency could maintain general situational awareness by monitoring developments in the field. The platform could serve as a forum for HEIs and research entities to exchange experiences in research security and discuss local, national, and international best practices. Concurrently, the implementation mandate of a research security officer should remain under the autonomous regulation of each HEI and research entity. Moreover, it is necessary to integrate research security aspects into the HEI risk matrix and to conduct regular internal self-assessments within research groups, departments, faculties and the entire organization, in accordance with the prescribed procedures.

Given that research security is based on both conducting a risk assessment and protecting one's own values, opinion leaders within academia (rectors, faculty deans, prominent researchers, respected lecturers, elected representatives to staff or student bodies, etc.) could position themselves as promoters of key principles among their peers and especially younger generations, who might be more susceptible to attractive bonuses offered by malicious foreign actors like China.

In addition, expert policy discussions can be held with government officials and politicians in the relevant parliamentary committees of the Riigikogu in order to attract attention to and raise awareness of the issue of research safety in general, to increase the willingness of state agencies and HEIs ' leadership to address the issue, and to reach a workable consensus on the establishment of a national framework for research safety in Estonia.

---

[160] ERR News. *10,000 People's Data Stolen in Genetic Testing Company Asper Biogene Leak*. ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1609194952/10-000-people-s-data-stolen-in-genetic-testing-company-asper-biogene-leak.

[161] ERR News. *Estonia declares Asper Biogene data theft leader an international fugitive*. ERR, 2024. Retrieved on December 16, 2024 from https://news.err.ee/1609548781/estonia-declares-asper-biogene-data-theft-leader-an-international-fugitive.

4. CONCLUDING RECOMMENDATIONS ON THE INSTRUMENTALIZATION OF RESEARCH SECURITY IN LATVIA AND ESTONIA

Before listing the recommendations, it is important to mention that all practices should be **regularly reviewed and updated**, which is at the core of best practice in research security. Thus, the most important recommendation is to invest in the **culture of security** within all included stakeholders of academia and the innovation ecosystem. Below are some general recommendations that can be implemented either individually or collectively at an organizational level as a single effort or joint initiative to enhance the research security of an individual or unit of an academic institution.

In light of the accelerated pace of technological advancement and the potential dual use of artificial intelligence, it is imperative to consider the necessity for prompt revisions to research security policies and practices. It is therefore crucial to establish a function within a HEI or research organization to monitor the state of developments and initiate the appropriate changes to mitigate the evolving threats.

Based on the risk analysis and best practices of risk mitigation, the recommendations for Latvia and Estonia countries are based on the 4Cs approach (4C - **C**ommitment, **C**ollaboration, **C**ommunication, and **C**ontrol).

The term **'commitment'** is defined as a formal agreement or public pledge to maintain and practice a security culture by highlighting relevant threat assessments and risk mitigation in the research agendas of the involved stakeholders. The term **'collaboration'** is used as an umbrella to describe the establishment of platforms and forums for the exchange of knowledge between government agencies and academic institutions, as well as within research organizations, with the aim of providing solutions that are in line with the latest developments. The term **'communication'** refers to a crucial process through which practical knowledge is transmitted and transformed from security-focused entities to research-focused organizations in order to increase threat awareness among institutions that are less informed and less engaged. The term **'control'** denotes a behavioral supervision strategy that is grounded in the expertise of duly qualified implementers, offering transparent guidance and templates to facilitate communication with researchers in a manner that is not in conflict with academic freedom.

The following recommendations are based on the gaps identified in **country analyses** and the best practices already implemented on different continents to reduce security risks in academia and research. These recommendations are founded upon the principle of commitment, which entails a joint responsibility.

4.1. Commitment

It would be beneficial for Latvia and Estonia to establish guiding frameworks of **formal and informal agreements** related to research security, while ensuring that **openness** and **transparency** are properly maintained. It is of paramount importance that research security policies do not fuel xenophobia or other forms of stereotypes or biases.

While enhancing the confidence of academia in international collaborations, national security requirements must be prioritized. It is essential to establish a common understanding between the various stakeholders in order to facilitate deconfliction of the disparate operational cultures of academia and security agencies. Given the significance of multilateral collaborations for scientific progress and innovation, it is vital to **safeguard both academic freedom and security** (of people and country).

Latvia and Estonia should continue to discuss and develop individual, institutional or even national policies to reduce security risks in academia and **promote research integrity practices**. As a commitment is an agreement or pledge to do something in the future, it should include review and updating is crucial when it comes to security practices; it is important to ensure that updates are based on **extensive feedback and evidence** (including whistleblowing channels).

The formulation of national and institutional research and innovation policies should encompass the consideration of a **range of security and safety concerns** pertaining to threat assessment and risk mitigation. Universities, research organizations and other academic institutions should develop **internal evaluation systems** to assess their research security and other safety practices, with a pre-planned external follow-up evaluation to track changes in implementation where necessary.

4.2. Collaboration

The spirit of partnership should be a key priority for the promotion of research security, supported by academic decision-makers, government stakeholders and other responsible bodies.

In collaboration with government authorities, a toolbox for HEI leadership, management and academic staff should be made available with the objective of identifying **common research security threats and risks to academic freedom**.

Regular and thorough **review of existing collaborative formats and partners** (including foreign donations, grants, gifts, equipment, etc.) and updating of public resources on active collaborations will promote responsible and transparent international research collaboration. A meaningful practice of self-disclosure and updating of conflicts of interest for academic staff should be considered.

A clear policy (including segregation of data) should be adopted regarding any potential academic collaboration with **an entity from a non-democratic regime**. Moreover, **complex or ambiguous ownership and partnerships should be investigated**; in the case of non-democratic regimes, both governmental and non-governmental collaborations may be subject to additional scrutiny.

Consideration should be given to **establishing inter-institutional formats to collaborate** on local practices in order to enhance the exchange of knowledge and experience. More attention should be paid to regional HEIs and research entities. Given that institutional leaders are best placed to promote a culture of security, it would be beneficial to develop and implement a dedicated format - the Research Security Awareness Program - to engage with the leadership and senior management of academic institutions and research organizations. This should be done on a regular basis in collaboration with other research security stakeholders.

A security-related agenda for international cooperation formats and partners could be facilitated by existing institutions, such as **national research councils and agencies**, which can be supported with relevant expertise and materials for public and institutional campaigns, as well as professional training and briefings.

Comprehensive research security would require a **segregation of duties**, as initial verification and screening could be carried out internally by academic institutions, following pre-established protocols, while further investigation and in-depth analysis should be outsourced to specialized security organizations as necessary.

In the context of **sensitive academia-government partnerships and cooperation in defense, security and foreign policy areas**, it is essential to prioritize those HEIs and research entities that

have robust security and safety measures in place and have no history of questionable collaborations with authoritarian regimes (e.g. Confucius Institute and other non-transparent ideological activities).

The establishment of the **Baltic Research Security Network of Practitioners** would be beneficial for regional coordination, cooperation and exchange of best practices for rapid information on due diligence issues and risk mitigation between the Baltic academic communities.

4.3. Communication

It is of the utmost importance to guarantee that non-democratic actors or their proxies are not influencing nor controlling the **general discourse or specific narratives** surrounding the issue of foreign malign interference and other forms of coercive activities within the academic community.

Common definitions, agreed in local contexts, are important to maintain cross-sectoral discussions on the balance between freedoms and restrictions, to reduce the sense of insecurity within academia while addressing **threats to national security**.

The implementation of **awareness campaigns** in public spaces on research security would prove advantageous in enhancing the knowledge of staff and students regarding potential risks. The core messages of these information campaigns emphasize the necessity of **safeguarding the principles of openness, transparency and equality** in academia, while maintaining a state of vigilance and preparedness to protect the material and non-material values.

Evidence-based information on investigated cases of **research security failures** can help to shape the professional and public agendas of various stakeholders and influence their decisions on resource allocation.

There should be clear communication within academic institutions and research organizations about the mandate of a **local focal point** for all internal security matters. In addition, the possibility of contacting **external security authorities** (e.g. through whistleblowing) should be established in order to streamline and protect communication flows when necessary.

It is recommended that HEIs, research organizations and other relevant stakeholders consider the development of either separate or **joint news bulletins** and **website sections** on their digital platforms, as well as email lists and other relevant resources for the circulation of publicly and internally materials and updates on research security issues in English and the national languages.

In designing and implementing **vertical and horizontal training** on various aspects of research security, it would be beneficial to consider the involvement of internal and external experts in order to expand the range of relevant cases and topics. Furthermore, briefings for the leadership and top management shall adhere to the principles of the **Train-the-Trainer approach** in order to ensure more effective communication on research security within academic institutions.

4.4. Control

It is essential to implement effective control measures to **safeguard critical assets** within HEIs or research entities, while ensuring that academic personnel involved in such matters receive the necessary guidance, training and protection. In order to safeguard critical assets, it would be prudent to consider and analyze the potential risks associated with **collaborative engagement with non-**

democratic regimes and implement appropriate preventive measures as advised by security authorities.

It is imperative that those engaged in the research process, and other personnel working on matters of a sensitive nature, are adequately trained to **recognize and avoid the use of elicitation techniques** that may be employed for the purpose of data collection.

It would be advisable to consider academic or research networking events in countries with a favorable or influential relationship with non-democratic regimes (e.g. China, Iran etc.) as **potentially dangerous venues** where HEI or research personnel may be exposed to influence or recruiting operations on a personal level.

In light of the proximity of geopolitically unstable actors and areas, it is i**mperative to implement comprehensive protocols for the physical protection of data servers** and the migration of data to secure environments in the event of kinetic aggression against an HEI or research entity.

Given that some research projects are dependent on access to **digital archives and databases**, it is imperative that regular comprehensive training on cyber hygiene, information management and data security is provided in order to foster a culture of research security at various levels: individual, institutional and national. In addition to HEIs and R&D entities, the fundamental principles of research security should also extend to archives, libraries, and museums that engage in academic collaboration.

It is recommended that **communication and other equipment** used by academic staff travelling to non-democratic destinations be monitored and controlled on a regular basis as a preventive measure to enhance the research security practice of data protection.

The design of **internal templates** (e.g., those pertaining to collaboration, travel, visitors, foreign allocations, etc.) should be based on the most recent threat criteria, include recommendations from relevant security services, and reflect contextualized risks for each HEI or research organization.

It would be erroneous to restrict the scope of risk assessment to the domains of hard science and technological innovations as developments in the **cognitive domain** present equally a significant challenge that cannot be ignored. Consequently, it is essential to consider the relevance of the social sciences and humanities with a particular focus on cognitive research, in order to identify emerging risks and to develop effective risk mitigation strategies.

A more nuanced and reasoned debate on **Confucius Institutes** and their activities in academia should be considered in public formats and within the framework of national security. Furthermore, in order to ensure the full transparency and integrity of Confucius Institutes, it is essential to implement **whistleblowing channels** that can detect and prevent any potential instances of censorship.

APPENDIX A. SOURCES AND METHODOLOGY

Semi-structured in-depth interviews have been conducted with the high-level representatives of the following organizations in Latvia and Estonia. The interview records have been anonymized and subjected to analysis in accordance with the research questions.

Latvia

Academia:

- Riga Technical University
- Vidzeme University of Applied Sciences
- Riga Stradins University

Government organizations and other non-academic entities:

- Latvian Research Council
- Latvian Ministry of Defense
- Latvian Ministry of Foreign Affairs
- Latvia's Constitution Protection Bureau

Two Latvian experts on China and national security been also interviewed in their professional capacity.

Estonia

Academia:

- University of Tartu
- Tallinn University of Technology (TalTech)
- Tallinn University
- Estonian Academy of Security Sciences
- Estonian Academy of Sciences

Government organizations and other non-academic entities:

- Estonian Ministry of Education and Research
- Estonian Ministry of Interior
- Estonian Research Council

Two Estonian experts on China have been also interviewed in their professional capacity.

APPENDIX B. QUESTIONNAIRE

This semi-structured anonymous interview is divided into four sections. The first section will address questions regarding ongoing collaboration with China and other non-democratic/authoritarian regimes. The second section will examine perceptions of security threats in academia. The third section will inquire about the institutional approach to mitigating risks and their experience with other academic or research entities. The fourth part of the interview will be aimed at elucidating the nature of ongoing government-HEI collaboration, including the identification of strategies to enhance collaboration for the purpose of safeguarding national security while ensuring the protection of academic freedom through the implementation of informed decision-making.

Part I (Foreign collaborations)

1. Is there any past or ongoing collaboration with Chinese universities or other research entities? Who initiated the collaboration?
2. Do you offer courses on China at the university? Do you have / had requests to establish Confucius Institute? Do you have cooperation with the Confucius Institutes in / outside the country? Who initiated this collaboration? Can you recall any (independent) Chinese study centers/think tanks in your country?
3. What about ongoing collaboration with China-friendly (or influenced) countries (with Chinese financial support)?
4. How many students have gone to China to study from your university? Any known scholarships / support / travel grants given by the university or the Chinese government?
5. Have you ever heard about the Thousand Talents program? What kind of faculty exchange (short-term visiting) programs are held each year with China, other non-democratic countries? What is the mandate for this kind of field visits?
6. Academic collaborations with foreign actors provide significant benefits for institutions. Have you rejected any prospective collaboration due to security related concerns?
7. Do you have students from China, Russia, or China-friendly (or -influenced) countries? If yes, what does the vetting procedure look like? What exchange projects / grants / programs are / were used? Have there been influence campaigns of any kind by the non-democratic government over the academics/students at the university? Any suspicious form of donations/scholarships/teacher exchange programs or even social media?
8. Have you experienced interest from the side of Chinese diplomats to visit your institution? (Recent visits if any? Follow-ups?).

Part II (Risks)

1. What could be among the main reasons in the country and for your institution to collaborate with Chinese scientists, universities, or research institutions?
2. What are the main risks you can name regarding international collaboration in higher education and research institutions with China and other non-democratic regimes? How do you evaluate the risks? Is there some internal and/or external mechanism of risk evaluation?
3. To your understanding, have these threats increased or decreased with the last 2-3 years?
4. Can you name any offers (public or private) you have received from non-democratic / authoritarian countries (joint courses, conferences, publications, students, centers, visits etc.)?

Part III (Mitigation / Institutional awareness)

1. Does your university have a risk management mechanism that covers international partnerships, including pre-cooperation risk analysis, partnership evaluation mechanisms and exit criteria? If yes, how are these mechanisms organized (please provide examples)?
2. How frequently do you inform the staff about potential risks? Do you have awareness training for the newcomers and interns?
3. Do you have research security training for staff (who is included, how frequently, does training include, who conducts)? Do you have monitoring mechanisms of risk mitigation?
4. Does your organization have international travel policies? (tracking, authorization for travel, equipment while traveling etc.). Do you have pre- and/or post-travel briefings? How do you ensure implementation of these policies?
5. How would you describe the level of security management at your institution? Did you had a different personal or institutional experience collaborating with other European or the US institutions?
6. Do you have a single Contact Point for knowledge / research security issue? If yes - since when? If no, do you consider / would it be helpful and what is needed to introduce it?
7. Do you have a vetting procedure for incoming visitors? What other verification strategies do you have?
8. Can you name any cases, when you / your institution benefited from increased awareness about risks and threats to research security?

Part IV (Government coordination)

1. Based on your experience, who is responsible for raising awareness of the risks associated with international academic cooperation in general and with specific (non-democratic / authoritarian) countries in particular?
2. Who do you consult internally and externally when you have doubts about the safety or security of international research cooperation? Do you have a focal point in governmental institutions? How would you describe / evaluate your cooperation with them? What should be done to improve it?

3. Do you see a role for the Ministry of Education and Research / Research Agency / other institutions (security related) in regulating the security of international academic cooperation between universities/research institutions and their counterparts?
4. Are there internal intervention and communication strategies for dealing with reputational risks and crisis situations related to international research cooperation? If yes - how is it organized, if no - how should it be organized?