https://doi.org/10.59862/k7m2x9q4r8/00

Foreword

The Research and Education Security Report, co-authored by a group of mostly European scholars, aims at analyzing and illustrating challenges, but to a degree also opportunities, connected with academia, research conducted by universities and other institutions, exchange of students and scholars, as well as abuses made by nation states benefiting from features of the research and education community. Understanding that academia cannot be isolated from external influences as it benefits greatly from openness to the world, researchers, students, and R&D sector managers should be aware of the kinds of risks that exist, and try to minimize them without violating basic principles of the broadly understood academia, hence openness to new ideas, new people, revolutionary developments, and contradictions that often bring inventions and provide progress.

The issue of security in research and education has been visible recently also due to rising geostrategic tensions, with Russia becoming an open enemy of the West (after invading Ukraine), China competing harshly with the United States in the technological war, often outpacing the latter in crucial, cutting-edge technologies, and Europe with massive implementation of certain solutions leaving the "Old Continent" behind in industrial potential and production. Such developments are connected with natural diffusion of technology or knowledge via joint research, study, merges and acquisitions, knowledge transfer, as well as with illegal or unethical behaviors, such as cyber-espionage and lab-espionage. Additionally, academia may be a cover

for the illegal activities of "students" or "researchers" operating under cover, as its openness and access to virtually all other spheres of economic, social, and political activities is broad. It also paves or simplifies the way to foreign information, manipulation, and interference campaigns (FIMIC), which are an important tool for influencing societies in democratic countries.

We are aware that the dynamic development of science observed in recent decades after the end of the Cold War has been made possible by globalization and the unrestricted exchange of ideas and scientific achievements. However, the current reality, where economic espionage is increasingly intertwined with state-initiated intelligence activities, is changing the perception of this openness. What was once the foundation for technological progress and innovation is now being viewed as a potential risk and threat. The growing rivalry between the United States and China, as well as tensions between democratic and authoritarian countries, are significantly affecting the academic world. Scientific openness, which has fueled international collaboration for years, is increasingly becoming one of the first casualties of this global competition.

Concerns about academic espionage are beginning to permeate processes related to research exchange, international grants, and scholarship programs. Viewing scientific collaboration through the lens of risk forces universities, security agencies, and the private sector to assess the potential benefits and dangers of international partnerships. Simultaneously, the advancing digitalization and dominance of cyberspace in many aspects of life have made the acquisition of confidential information easier than ever before, further intensifying the challenges facing the academic community.

The advancing digitalization and growth of cyberspace also introduces new threats to the security of scientific research, including cyber-attacks, infiltration, and espionage, which endanger data, research results, and the safety of researchers. Examples of such incidents, such as phishing attacks, data theft attempts, and global cyber-espionage campaigns highlight particular risks to strategic fields such as artificial intelligence development, biotechnology, and defense technologies. Infiltration by Chinese and Russian entities and the use of research results for military or terrorist purposes

further emphasize the need to protect universities and scientific institutions. While numerous protective measures have already been implemented in the United States, Europe still lacks comprehensive actions in this area. Polish universities, despite their significant research potential, face financial constraints and a growing need for state support to ensure security.

We present to you a report that is the result of the Research and Education Security (RES) conference organized by the Centre for International Studies and Development (CISAD), held on December 5, 2024, in Krakow, Poland. The conference and the reports resulting from it focused on various aspects of the safety of academic research and related data safety in the turbulent time of emerging conflicts and hybrid war activities after the relative calm period following the end of the Cold War. The reports cover various aspects of research activities and each report is accompanied by a set of recommendations which if implemented should increase the safety level of the research, research results, and engaged academic personnel.

The conference participants discussed the techniques and instruments of intelligence used to penetrate the research environment, such open data collection, personal intelligence, electronic intelligence and agents of influence, the way they are used in intelligence activities, and the threats they represent to academia. The question of research data and activities, its legal division and protection of respective subdivisions, was also considered from the point of view of international law. It included conclusions from the war in Ukraine and compared the legal situation with its practical reflection in everyday practice.

Basic issues of keeping balance between academic freedom and research safety were delineated in a few of the reports. They describe the dilemma between attempts to secure the research process itself, its integrity, and its outcomes on one side, and the need to cooperate worldwide to facilitate and accelerate the academic progress on the other, as well as possibilities for cooperation between the academic community and intelligence organizations within the same country or a group of allied countries. The same set of issues apply to the transfer of information and technology related to academic research. It reflects the same set of contradicting aspects, such as the need to

cooperate but also the risk of data leakage to unwanted actors. The relation of research cooperation between institutions and nations, and the need to make sure the research results are safe and cannot be used by third parties without the researchers' permission is crucial. The complexity of the situation is growing together with rising tensions between global powers.

A separate particularity of today's academic environment is its interlocking with widely understood ethics and the need to protect some of the participants, especially students. The practical and ethical challenges faced by scholars and university lecturers while conducting research related to China or including its results into the teaching process, especially in the case of student groups containing students from Mainland China and potential threats to both the students and the teachers, were used as an example of the issue. Academic institutions are exposed to trans-national repressions orchestrated by the Chinese Communist Party (CCP), which target both students and scholars in universities and research institutions. They not only influence Chinese students and researchers abroad but also their families in China. In one of the reports, we also find a description of how the CCP tries to control the flow of information directed toward Chinese students abroad.

Students from other countries are also targets of disinformation campaigns while studying abroad. After they are placed in a new and unknow environment they can be easily influenced by social media platforms if their countries of origin or other organizations are able to spread content supporting their vision of the host country, which may not be true but inspires the audience's confidence.

Cybersecurity in academic research and especially cyber-attacks on academic institutions were discussed separately, including statistics of recent attacks and its threat to both intellectual property and national security. The topic is especially important as the authors took into consideration recent Russian and Chinese malicious cyber-activities targeting academic institutions, its statistics and results regarding the types of academic institutions involved, their field of research, geographical location, and the statistics and character of the malicious activities. The physical security of the servers and other infrastructure is another issue, especially in places where there are

combat activities such as Ukraine. Currently, cybersecurity is understood not only as the risk of losing data but also to let external actors influence one's research or even the object of the research.

Space and satellite security is an important topic because depending on the circumstances they may constitute both a laboratory that enables experiments in an environment unavailable on the Earth's surface to be conducted or the communication tools needed to communicate its course and results. In the case of such objects, the security issues become even more complex as they may be disturbed by some third-party actors and damaged by natural factors independent from human beings.

Some reports focus on a specific policy, set of practical or legal regulations, or a real-life case study. One report analyzes the issue of technological standardization in China, describing its recent development and how it is used to promote Chinese values. It also provides several standardization solutions that China either attempted to promote or successfully promoted to be used worldwide.

The Taiwan case study introduces the People's Republic of China's (PRC) attempts to influence the Taiwanese academic research environment using technological tools and human factors. In this specific case, research security is strictly connected with national security, which results in the involvement of state factors from both sides of the Taiwan Strait, and the procedures developed by the Taiwanese side should be analyzed as a lesson for the EU countries.

The US and its 2018 "China Initiative" may also be considered as a pattern to follow in the EU, when academic institutions cooperate with other public and private institutions, Chinese factors are included directly or more often indirectly or undisclosedly, and the research results have to be secured from unintentional transfer to Chinese institutions.

A long list of discussed issues is sealed with the first-hand story of a collaborator of Russia's spying services anchored deeply in the Estonian academic environment as an agent of influence participating in everyday academic life over a long period of time until he was finally detained and sentenced.

*

The report is divided into four thematic sections dedicated to: i*ntelligence in academia*, *cybersecurity and technological security in research*, *case studies: China's and Russia's influence*, *and knowledge security and research ethics*. Below you will find a summary of the recommendations derived from each text included in this volume. Full descriptions, along with the texts outlining their origins, can be found in the subsequent sections of the report.

The first section of the report is devoted to the issue of challenges and opportunities connected to intelligence problems in academia, which is an under-researched area, but due to academic openness and sophistication is at risk of espionage. The first chapter by **Niklas Swanström** and **Filip Borges Månsson**, entitled **Balancing Security and Innovation: A Policy Perspective**, describes the increasingly complex security-innovation nexus, as nations balance protecting national interests with fostering technological advancement. The authors explain why rising cyber-threats from authoritarian states heighten security concerns, challenging international research cooperation. They stress the fact that adaptive regulations, stronger intellectual property laws, and investment in emerging technologies are crucial for safeguarding innovation while maintaining security. This is followed by an analysis by **Artur Gruszczak**, **Academic Espionage: Finding a Better Balance between Open Science and Security Imperatives**. The author describes the way academic institutions face escalating threats from cybercrime, espionage, and unauthorized use of research outcomes, necessitating greater security measures. He stresses the fact of certain governments and private actors targeting universities to access economically and strategically valuable intellectual property, which results in threatening academic freedom. At the end of the chapter, a conclusion is drawn that critical balance must be set up between promoting openness and implementing rigorous risk management to safeguard intellectual integrity and innovation. In the third chapter, entitled **Cybersecurity in the Academic Environment: Scientific Institutions as Targets of Cyber-Attacks**, **Andrii Davydiuk** focuses on cyber-attacks on academic institutions exposing them to risks such as data breaches, operational disruptions, and intellectual property theft. He explains why the creation of

tailored cybersecurity profiles, regular training for staff and researchers, and partnerships with governments and global organizations are essential to enhance resilience. He also stresses that investment in secure infrastructure and proactive risk assessments is crucial to protect research and national security interests. The fourth chapter by **Aleksi Kajander**: **Research Data during an Armed Conflict: An Overlooked Target?** describes how digital research data lacks and respective legal protection under International Humanitarian Law (IHL) during armed conflicts, and how this leaves academic institutions vulnerable to exploitation. It is stressed that universities must raise awareness about these risks and advocate for reforms to address the legal loopholes and secure research data in conflict scenarios, which is critical to preserving intellectual assets and protecting academic institutions.

The second section of the report deals with a problem that has recently been especially visible, namely the issue of cybersecurity and technological security in research. It is opened with an analysis by **Sławomir Wyciślak**, **A Systemic Approach to Cybersecurity in International Research Projects. The Role of Digital Platforms**. This chapter stresses the need of academic institutions to adopt a systemic approach to tackle cybersecurity challenges and to address vulnerabilities in research workflows and digital platforms. It also explains why building a robust security culture should involve regular training, awareness campaigns, and implementing advanced cybersecurity tools, and why institutions must align risk management strategies with their operational goals to protect research integrity and foster safe international collaboration. A broader perspective of cybersecurity in academia is provided by **Izabela Albrycht** in the chapter, **Cyberthreats to the Science and Research Sector as a Challenge to National Security and Economic Competitiveness**. The analyst writes how the academic sector is increasingly targeted by cyber-attacks, which causes risks to critical data, intellectual property, and operational continuity. She comes to the conclusion that establishing EU-wide and national cyber-resilience programs is essential to provide financial support, training, and governance frameworks. At the same time, long-term strategies must include scalable security solutions, sustainable funding, and mechanisms to share best practices across institutions. In the eighth chapter, devoted to: **Safety and**

Security of Space-Enabled Education/Learning and Research, **Marek Czajkowski** explains why space-enabled research faces growing risks from space debris, collisions, and geopolitical conflicts. He states that mitigating threats such as the Kessler syndrome requires immediate international cooperation to manage space debris and ensure safe operations. He concludes that it is essential to sustain space-based research, necessitates policy-driven safety measures, and the coordination of efforts to protect the integrity of satellite-based systems. Finally, **Paweł Frankowski** contributes with the chapter, **Knowledge Without Borders: Securing Technology and Data in Global Academic Collaboration**, which stresses that global academic collaboration requires stringent measures to mitigate risks such as data breaches and inconsistent security practices. The text explains why an EU-level due diligence agency and resource-sharing frameworks are vital to address these vulnerabilities, while universities must at the same time strengthen cross-border partnerships and adopt consistent procedures to ensure secure knowledge transfer.

The third part of the report is illustrated with numerous case studies, devoted to China's and Russia's influence, hence, the most important non -Western players on the global map. The tenth chapter by **Marcin Przychodniak**, **The US "China Initiative" in the Face of Challenges in Scientific and Research Cooperation with the People's Republic of China. Relevance to the EU**, explains how the US "China Initiative" addresses threats from Chinese activities in academia and how it offers insights for EU efforts to secure institutions. Despite political controversies, its focus on advisory roles and public-private collaborations highlights effective measures for research protection. The author comes to the conclusion that adapting similar initiatives could bolster the EU's defense against comparable challenges. It is followed by Błażej Sajduk's analysis, The Importance of Technological Standards in Chinese Foreign Policy. The author analyzes how China uses technological standards strategically to exert influence globally through initiatives such as the Belt and Road Initiative. He stresses the extent to which this approach poses risks of technological dependency and undermines institutional autonomy in academia. He concludes that promoting open standards and bolstering technical expertise within universities is essential to counteract

these geopolitical maneuvers. Subsequently, **Vladimir Sazonov's Russian Influence Activities and Espionage in Estonian Academic Environment: The Case of Viacheslav Morozov, a Russian GRU Spy at the University of Tartu**, explains the case of GRU spy Viacheslav Morozov and how it demonstrates the risks of espionage within academic institutions. The text tells the story of how Morozov used his position to spread pro-Kremlin narratives and gather intelligence, and as a result it underlines the need for counterintelligence measures. The author comes to the conclusion that universities must adopt stricter vigilance and policies to prevent this kind of infiltration and safeguard academic integrity. In the final chapter in this section, authored by **Marcin Jerzewski**, and entitled **Situating Academia in Economic Security Strategies: Lessons from Taiwan**, the author describes how Taiwan's research security regime safeguards national technologies from Chinese influence amid cross-strait tensions. He analyzes the recent legislative amendments which enhance protection against espionage and influence operations linked to China. He stresses that integrating research security into national frameworks and supporting grassroots initiatives are vital for resilience.

The final section of the report is devoted to knowledge security and research ethics. In the first contribution to this section, **Eliza Kotowska** deals with the problem of: **Addressing Disinformation Vulnerabilities in International Students and Paths to Resilience**, explaining how international students are susceptible to disinformation due to social isolation, unfamiliar political contexts, and language barriers. As a solution she suggests that universities can combat this by offering media literacy training, creating fact-checking resources, and fostering social integration. Collaboration with fact-checking organizations and culturally inclusive initiatives can also strengthen resilience against disinformation campaigns. In the following chapter, **Knowledge Security: A New Policy Concept for Science and Politics**, **Leo Eigner** provides an analysis on how knowledge security emphasizes balancing openness with the protection of research assets and national competitiveness. He stresses that democratic nations must develop frameworks to safeguard intellectual contributions while promoting collaboration, and at the same

time policy recommendations should enable identifying vulnerabilities, aligning international research security, and adhering to ethical standards. The issue of **Decolonizing Knowledge: The Practical and Ethical Challenges of Researching "Sensitive" Topics in and about China**, is analyzed by **David O'Brien**. The researcher explains that engaging with China's politicized academic environment requires resisting self-censorship and maintaining ethical research standards. He stresses that open dialogue and mutual challenges are necessary to uphold universal academic values and that researchers must navigate collaborations carefully to avoid compromising integrity while supporting constructive discourse. Finally, **Melissa Shani Brown's** chapter on **Internationalization, the Securitization of Knowledge, and Trans-National Repression within and beyond the Classroom**, explains why trans-national repression (TNR) poses significant challenges to the safety and freedom of international academic communities. She comes to the conclusion that universities must implement policies to address TNR, safeguard vulnerable groups, and ensure academic freedom. Strategies should include awareness programs, protective measures, and collaboration with human rights organizations to counteract surveillance and intimidation.

The list is not a complete analysis of all risks and challenges connected with research and education security, but it aims at analyzing issues that are particularly relevant and important in Central and Eastern Europe, while also influencing the global research community. We must be aware that new challenges appear every day, but despite them, we cannot resign from the basic principles of research, including its openness and ethics, while being aware of new risks appearing.

At the end of this short introduction, we would like to show our appreciation to the Ministry of Science and Higher Education for supporting financially and patronizing the conference.The organization of the event and preparation of this Report was possible only thanks to that support.

The editors would like to thank all the people who have been engaged in the Research and Education Security project, including participants of the Research and Security Conference in December 2024, contributors to the Report, as well as the team at the Centre for International Studies and Development of

the Jagiellonian University, including Weronika Krupa (administrative coordinator), Monika Klecka, Karolina Kaczmarczyk, Dr. Łukasz Stach. Krzysztof Stefan, and Katarzyna Sypień. It is also important to mention the editors at the AT Wydawnictwo (AT Publishing House), especially Dr. Adrian Gorgosz (editor-in-chief) and Hayden Berry (proofreader). We are grateful for the representatives of the Ministry of Science and Higher Education, especially Angelika Instunajd-Łącka and Piotr Kowalczyk. Without them, it would not be possible to complete this report.

Marcin Grabowski, Piotr Kwiatkowski, Błażej Sajduk