RESEARCH AND EDUCATION SECURITY

REPORT

EDITED BY
MARCIN GRABOWSKI
PIOTR KWIATKOWSKI
BŁAŻEJ SAJDUK

ATW

UNIWERSYTET JAGIELLOŃSKI W KRAKOWIE

Ministerstwo Nauki i Szkolnictwa Wyższego

Minister Nauki

WSMiPUJ UCZYMY ROZUMIEĆ ŚWIAT

CISAD CENTRE FOR INTERNATIONAL STUDIES AND DEVELOPMENT

Research and Education Security Report

Research and Education Security Report

Edited by
Marcin Grabowski, Piotr Kwiatkowski, Błażej Sajduk

Research and Education Security Report

Publishing review
Dr hab. Robert Kłaczyński, prof. UKEN
Dr hab. Jakub Zajączkowski

Scientific editors
Marcin Grabowski
Piotr Kwiatkowski
Błażej Sajduk

Proofreading
Hayden Berry

Managing editor
Adrian Gorgosz

Layout
Maciej Kwiatkowski

Book cover
Weronika Krupa

ISBN: 978-83-68278-11-8

https://doi.org/10.59862/k7m2x9q4r8

This publication is financed from the budget of the Polish Ministry of Science and Education as part of the implementation of the task entitled ‘Organization of the Conference: Research and Education Security (RES)’

Minister of Science and Higher Education
Republic of Poland

Contents

IV.

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

PART I.

INTELLIGENCE: CHALLENGES AND OPPORTUNITIES IN THE ACADEMIA

https://doi org/10 59862/k7m2x9q4r8/01

Chapter I

Balancing Security And Innovation: A Policy Perspective

NIKLAS SWANSTRÖM
Director at the Institute for Security & Development Policy (ISDP)*
ORCID 0000-0003-2326-4634

FILIP BORGES MÅNSSON
MA Student at the Military History Department of the Swedish Defence University
ORCID 0009-0006-0681-279X

Abstract: This paper examines the evolving tension between fostering open, collaborative innovation and safeguarding national, economic, and induvial security in an era marked by rapid technological change and increasingly assertive authoritarian actors. Through an analysis of emerging technologies, including Artificial Intelligence (AI), quantum computing, biotechnology, and the internet of things (IOT's), we highlight how innovation simultaneously strengthens and undermine security. The paper concludes by offering a series of policy recommendations aimed at enabling governments to protect critical assets, maintain strategic autonomy, and preserve the benefits of international research cooperation without compromising security.

Keywords: Security, innovation, quantum computing, IP, biotechnology, AI, cybersecurity, dual-use technology, OSINT, cooperation

* Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI)

Policy

In the 21st century, the dual imperatives of maintaining security and fostering innovation have become increasingly intertwined and complex. As nations strive to protect their citizens, infrastructure, and economic interests, they must simultaneously cultivate an environment encouraging technological advancement and creative problem-solving. Much of this innovation is based on international cooperation, exchanges of researchers ranging from basic research at universities to high tech research institutions. These exchanges are crucial for innovation but increases the risk of brain drain, Intellectual Property (IP) theft, and enhances the abilities of hostile states. This delicate balance between security and innovation is crucial for national prosperity, competitiveness, and long-term stability.

Authoritarian states have increasingly been associated with hostile actions in research and innovation, ranging from IP theft to hostile takeovers of companies. China has been noted as one of the most active and successful states when it comes to threats to the European science and innovation security, but simultaneously crucial for some of Europe's innovation and supply chain in sectors such as green technology and rare earth minerals.[1]

The rapid pace of technological change has created new vulnerabilities and security challenges, from sophisticated cyber threats to the potential misuse of artificial intelligence and biotechnology. Concurrently, these same technological advancements offer unprecedented opportunities for economic growth, improved quality of life, and solutions to global challenges such as climate change and healthcare crises. It has famously been noted that expanded supply chain dependency has been the core of our economic development, but also our increased insecurity and dependency on authoritarian states such as Russia and China. Similarly in research and innovation, there would not have been such a rapid progress without the free exchanges of research and innovation, but at the same time it has been misused by authoritarian states that have stolen individual researchers' products, but more importantly put European nations at risk and in a dependency position toward such authoritarian states.

[1] Niklas Swanstrom, Fredrik Erixon and Mrittika Guha Sarkar, *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies,* (Armin Lear Press 2024).

This paper aims to provide a comprehensive framework for understanding and addressing the tension between security and innovation, and to examine how we best can secure both innovation and security. By examining current trends, and drawing insights from various sectors, we seek to offer practical policy recommendations that can help strike an optimal balance.

The following sections will delve into the intricate relationship between security and innovation, explore the current global landscape, and propose strategies for policymakers to navigate this complex terrain. Our goal is to contribute to the development of policies that not only protect against current and future threats but also unleash the full potential of human ingenuity and technological progress.

The Security-Innovation Nexus

In today's interconnected world, the concept of security has expanded far beyond traditional notions of military defense. It now encompasses a wide range of domains, including, but not limited to:

a. Cybersecurity, which involves protecting digital infrastructure, data, and online systems from attacks and unauthorized access.
b. Economic security, focusing on safeguarding national economic interests, intellectual property, and critical industries.
c. National security, aiming at defending against both conventional and unconventional threats to sovereignty and national interests.
d. Individual security, which focuses on protecting individuals from IP theft, economic sustainability, and social security.
e. Environmental security, addressing climate change and other environmental challenges that pose risks to stability and well-being.
f. Health security, which aims at protecting populations from pandemics and other health crises.

This multifaceted nature of security requires a holistic approach that considers the interplay between various domains and the role of innovation in both creating and mitigating risks. The challenge many times is that there is separate legislation and understanding between the fields as well as a diversified political spectrum with opposing political views, something that might not be the case in regard to malign actors. Notably there are very different perspectives on what is important in each state. Europe would, as one example, focus on individual security, while China would disregard that aspect and focus on national security. This is something that will increase the challenges in terms of solutions to many of the problems, such as regulations of artificial intelligence (AI) and quantum computing. Many of the different focuses could also be perceived to be in conflict with each other, such as environmental and economic security.

The Role of Innovation in Economic Growth and National Competitiveness

Innovation stands as a fundamental pillar of modern economic development and national competitive advantage. In today's rapidly evolving global landscape, a nation's capacity to innovate has become increasingly crucial in determining its economic prosperity, international standing, and security, and history has shown that innovation is best done without interference of government regulations.[2] Innovation drives economic growth, enhances productivity, strengthens national competitiveness, and enables states to address critical societal challenges; failure to innovate leads to economic stagnation or decline.

Innovation has always served as a powerful engine of economic growth by creating new industries, products, and services while transforming existing ones. When organizations and individuals develop novel solutions to market needs, they generate new economic opportunities that ripple throughout the economy. This process creates jobs, stimulates investment, and generates wealth across multiple sectors. Innovation-driven growth is particularly valuable because it often creates high-skilled, well-paying positions that contribute to the development of a knowledge-based economy. That said, it is dangerous to focus only on innovation and outsource production, as that also creates a dependency that could be challenging, especially as innovation

[2] Philippe Aghion, Antonin Bergeaud and John Van Reenen, "The Impact of Regulation on Innovation," *Cato Institute*, April 19, 2023, https://www.cato.org/research-briefs-economic-policy/impact-regulation-innovation.

and research can be obtained by illegal or legal means, as theft or hostile takeover of companies.[3]

The economic impact of innovation extends far beyond direct effects. When companies introduce innovative products or processes, they often create positive externalities that benefit the broader economy. These spillover effects can include knowledge transfer between industries, the development of supporting sectors, and the creation of new market opportunities for other businesses. Furthermore, innovative activities tend to cluster geographically, leading to the development of innovation hubs that attract talent, investment, and additional innovative enterprises.[4]

Additionally, innovation plays a crucial role in driving productivity growth, which is essential for long-term economic prosperity. Through technological advancements and process improvements, organizations can produce more output with the same or fewer inputs, leading to increased efficiency and reduced costs. This productivity enhancement occurs through various channels, including automation of routine tasks, optimization of production processes, and implementation of more effective management practices.

The impact of innovation on productivity is particularly evident in the digital age. Digital technologies and their applications have revolutionized how businesses operate, enabling unprecedented levels of efficiency and creating new possibilities for value creation. Cloud computing, artificial intelligence, and the Internet of Things have become powerful tools for productivity enhancement, allowing organizations to streamline operations, make data-driven decisions, and better serve their customers.

In the international arena, innovation has become a key determinant of national competitiveness. Countries that foster strong innovation ecosystems typically enjoy advantages in international trade, attract more foreign investment, and maintain higher standards of living for their citizens. A nation's innovative capacity depends on its ability to develop and maintain effective

[3] Swanstrom, Fredrik and Guha Sarkar, *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies.*

[4] McKinsey & Company, "A Playbook for Innovation Hubs and Ecosystems," *Global Institute for Innovation and Development*, February 28, 2023, https://giid.org/app/uploads/2024/03/A-playbook-for-innovation-hubs-and-ecosystems-McKinsey.pdf.

national innovation systems—complex networks of institutions, policies, and practices that support the creation and diffusion of new technologies and knowledge.

Successful national innovation systems typically feature strong collaboration between academia, industry, and government. Universities and research institutions generate new knowledge and train skilled workers, while businesses transform innovations into marketable products and services. Governments play a crucial role by funding basic research, establishing supportive regulatory frameworks, and ensuring adequate protection of intellectual property rights.

The COVID-19 pandemic demonstrated the critical importance of innovation in addressing global challenges. The rapid development of vaccines, adaptation of business models, and creation of new digital solutions showcased how innovation can help societies respond to unprecedented challenges. This experience highlighted the value of maintaining robust innovation capabilities as a form of societal resilience, and it also highlighted the dangers of being dependent on foreign innovations.

Looking forward, the pace of innovation is likely to accelerate, driven by advances in fields such as AI, biotechnology, and quantum computing. Nations that wish to maintain or enhance their competitive positions must continually adapt their innovation strategies to address emerging challenges and opportunities. This includes ensuring that innovation efforts are sustainable, inclusive, and aligned with societal values.

Innovation remains essential for economic growth and national competitiveness in an increasingly complex global environment. Success in the innovation economy requires a sustained commitment to building and maintaining effective innovation ecosystems, fostering collaboration across sectors, and ensuring that innovation efforts address economic and societal needs. As the world faces unprecedented challenges and opportunities, the ability to innovate effectively will become even more crucial for national success and societal well-being.

The Tension Between Security and Innovation

The relationship between security and innovation presents one of the most complex challenges in modern policymaking. While both elements are fundamental to national prosperity and development, they often appear to work at cross-purposes, creating what many observers describe as an inherent tension.[5] This contribution explores the multifaceted nature of this tension, its implications for various stakeholders, and potential approaches to managing these competing demands.

The apparent conflict between security and innovation stems from their fundamentally different orientations toward risk and change. Security, by its nature, seeks to protect, preserve, and maintain stability. It emphasizes controlled environments, predictable outcomes, and risk mitigation. Innovation, conversely, thrives on disruption, embraces uncertainty, and often requires challenging established norms and practices, and not to mention cross-border cooperation in complex environments.

This divergence manifests in practical tensions across various domains. In organizational settings, security protocols may restrict access to resources or information that could fuel innovative thinking. In technological development, security requirements might constrain the exploration of novel solutions or limit the ability to rapidly iterate and test new ideas. At a national level, security considerations might influence research funding priorities or restrict international collaboration opportunities that could drive innovation.

The tension between security and innovation is perhaps most evident in approaches to risk management. Security frameworks typically adopt a preventative stance, seeking to identify and mitigate potential threats before they materialize. This approach often leads to the implementation of strict controls, detailed documentation requirements, and multiple layers of oversight.[6] While these measures serve important protective functions, they can create significant barriers to innovation, which often requires rapid

[5] Jack Corrigan, Melissa Flagg and Dewey Murdick, "The Policy Playbook," *Center for Security and Emerging Technology* (2023): 8–9, https://doi.org/10.51593/20230018.

[6] Forbes Technology Council, "Benefits And Cautions Of Aligning With Cybersecurity Frameworks," *Forbes*, February 13, 2024, https://www.forbes.com/councils/forbestechcouncil/2024/02/13/benefits-and-cautions-of-aligning-with-cybersecurity-frameworks/.

experimentation, acceptance of failure, and the ability to pivot quickly based on new information or opportunities.

The challenge of balancing these competing approaches to risk becomes particularly acute in sectors such as cybersecurity, biotechnology, and AI, where innovation capabilities directly impact security outcomes. Organizations and policymakers must grapple with questions of how much risk is acceptable, how to evaluate potential benefits against potential threats, and how to create frameworks that protect essential interests without stifling beneficial innovation.

Another critical dimension of the security-innovation tension involves the management of information and knowledge. Innovation typically flourishes in environments characterized by open exchange of ideas, cross-pollination of concepts, and broad collaboration across different domains and organizations. Security considerations, however, often necessitate restrictions on information sharing, implementation of need-to-know protocols, and limitations on external collaboration.

This tension becomes particularly pronounced in research and development settings, where breakthrough innovations often emerge from unexpected connections and cross-disciplinary and cross-border insights. Security requirements that compartmentalize information or limit external engagement can inadvertently create silos that impede creative problem-solving and innovation. The challenge extends to international collaboration, where security concerns about technology transfer or intellectual property protection must be balanced against the benefits of global innovation networks. This is not least a concern realizing that IP theft and espionage in academic and commercial settings.

The allocation of limited resources presents another significant manifestation of the security-innovation tension. Organizations and nations must make difficult decisions about how to distribute financial, human, and technological resources between security initiatives and innovation programs. These decisions are complicated by differences in how security and innovation investments are evaluated and measured.

Security investments often focus on preventing negative outcomes and establishing defenses against intrusion, making their value difficult to quantify directly. Innovation investments, while potentially offering higher returns, come with greater uncertainty and longer time horizons for realizing benefits.[7] This asymmetry in evaluation metrics can lead to bias toward security investments, particularly in risk-averse organizations or during periods of heightened security concerns.

The tension between security and innovation, while real, need not be viewed as an insurmountable obstacle. Success in the modern environment requires developing sophisticated approaches that can accommodate both imperatives. This demands careful attention to institutional design, policy frameworks, and organizational culture, as well as recognition that security and innovation can, in many cases, be mutually reinforcing rather than exclusively competing priorities.

Moving forward, the key challenge for leaders and policymakers will be to develop nuanced approaches that can protect essential security interests while maintaining the flexibility and openness necessary for innovation to flourish. This requires ongoing dialogue between security and innovation stakeholders, creative approaches to risk management, and commitment to finding balanced solutions that serve both immediate security needs and longer-term innovation goals.

Innovation Trends and Their Security Implications

The rapid pace of technological innovation is fundamentally reshaping our world, bringing both unprecedented opportunities and complex security challenges, at a rapidly increasing phase. As emerging technologies transform industries and societies, they create new vulnerabilities and threats while simultaneously offering novel solutions to security challenges, even if the creation of a secure environment is too often reactive rather than proactive. This segment explores the intricate relationship between major innovation trends and their security implications, examining how these developments are reshaping our approach to security in the modern age.

[7] ISACA, "Quantifying information risk and security," *ISACA Journal*, July 1, 2013, https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security.

Artificial Intelligence and Machine Learning: Reshaping Security Paradigms

The emergence of AI and machine learning represents perhaps the most transformative technological shift of our era, fundamentally altering the security landscape. In the defensive realm, AI systems are revolutionizing threat detection and response capabilities. Advanced machine learning algorithms can analyze vast amounts of data to identify patterns indicative of security threats, enabling proactive rather than reactive security measures. These systems are particularly powerful in cybersecurity, where they can detect anomalies and potential attacks in real-time, often identifying threats that would be impossible for human analysts to spot.

However, the same capabilities that make AI powerful for defense also create significant security concerns. Adversaries can leverage AI to develop more sophisticated attack methods, from advanced malware that adapts to defensive measures to deep fakes that can deceive even careful observers. The potential for autonomous weapons systems raises profound ethical and security questions about the role of human judgment in military decisions and the possibility of uncontrolled escalation in conflicts. Moreover, AI still possesses the inherent flaw that it can still be biased and prone to make mistakes, notably in terms of machine learning. Slight alterations can have profound consequences, potentially resulting in the AI being used in an unauthorized manner and as a tool for theft, misuse, and manipulation of data by adversaries.[8]

The Internet of Things: The Challenge of Securing a Connected World

The proliferation of Internet of Things (IoT) devices is creating a more connected and intelligent world but also introducing new security vulnerabilities at an unprecedented scale. Smart city technologies offer tremendous potential for improving public safety and emergency response through better monitoring and coordination of urban systems. Connected sensors and devices

[8] OECD, "Assessing potential future artificial intelligence risks, benefits and policy imperatives," *OECD Artificial Intelligence Papers*, No. 27 (2024): 19–25, https://doi.org/10.1787/3f4e3dfb-en.

can provide early warning of natural disasters, monitor critical infrastructure, and optimize emergency services deployment.

Yet the massive expansion of connected devices creates an equally massive attack surface for cyber threats. Many IoT devices lack robust security features, making them vulnerable to compromise. The interconnected nature of IoT systems means that a breach in one component can potentially compromise entire networks. Privacy concerns are particularly acute, as IoT devices collect vast amounts of personal and behavioral data that could be exploited by malicious actors.[9]

5G and Beyond: The Infrastructure of Future Security

The deployment of 5G, and 6G, networks and the development of future telecommunications technologies promise to transform security capabilities through enhanced communication and data processing capabilities. These networks will enable new applications in emergency response, surveillance, and security monitoring, with the potential for real-time coordination of complex security operations. The increased bandwidth and reduced latency of 5G networks could revolutionize everything from drone operations to remote medical procedures.

However, the fundamental role of these networks in critical infrastructure creates significant security concerns. The complexity of 5G networks introduces new vulnerabilities that could be exploited by sophisticated attackers.[10] Concerns about foreign technology providers and the potential for built-in backdoors or vulnerabilities have made 5G deployment a matter of national security debate in many countries. The need to secure these networks while maintaining their performance benefits presents a major challenge for security professionals.

[9] CISA, NSA, FBI, NCSC-UK, ACSC, CCCS and NCSC-NZ, "Cybersecurity Best Practices for Smart Cities", April 19, 2023, https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

[10] Tom Wheeler and David Simpson, "The digital future requires making 5G secure," *Brookings Institution*, December 12, 2022, https://www.brookings.edu/articles/the-digital-future-requires-making-5g-secure/.

Looking Beyond 5G, the anticipated deployment of 6G networks will continue to redefine connectivity standards and have transformative implications for society and security alike. As it will most likely integrate even deeper with AI and IoT, the need to ensure and address the current challenges we face with 5G is essential as the risks of privacy intrusions, data exploitation, and network manipulation by malicious actors will continue to pose significant challenges and may grow exponentially, as new network iterations such as 6G is likely have its own intricate flaws once developed and deployed.

Quantum Computing: The Next Frontier of Cryptographic Security

Quantum computing represents both a revolutionary advance in computational capabilities and a fundamental challenge to current security paradigms. The potential of quantum computers to solve complex problems could transform fields ranging from drug discovery to climate modeling. In the security domain, quantum computing offers the possibility of unbreakable encryption methods and advanced threat detection capabilities, but reversely also unbreakable threats to individual and government security.

However, the same computational power that makes quantum computers revolutionary also threatens to render current encryption methods obsolete. The ability of quantum computers to factor large numbers quickly could break many current cryptographic systems, potentially exposing sensitive data and communications. This has sparked a race to develop quantum-resistant cryptography before practical quantum computers become a reality.

Moreover, the implications of quantum computing extend beyond cryptography and pose challenges to broader aspects of cybersecurity infrastructure. Notably, blockchain technologies, widely considered secure due to their reliance on asymmetric cryptography, could potentially be undermined by quantum decryption capabilities.[11] The global race to harness quantum computing is also intensifying geopolitical tensions, as nations seek to develop quantum technologies for both defensive and offensive purposes. In this con-

[11] Deloitte, "Quantum computers and the Bitcoin blockchain," *Deloitte Netherlands: Risk Advisory Perspectives*, 2023, https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.

text, the emergence of "quantum supremacy"—the point at which quantum computers surpass classical computers in solving specific tasks—could reshape power dynamics in both commercial and military domains.

Biotechnology and Synthetic Biology: The Frontier of Biosecurity

Advances in biotechnology and synthetic biology are revolutionizing our ability to understand and manipulate biological systems. These capabilities have demonstrated their value during the COVID-19 pandemic, enabling rapid vaccine development and new approaches to disease detection and treatment. The potential for personalized medicine and advanced diagnostic tools offers tremendous promise for public health and security.

Yet these same advances raise serious biosecurity concerns, notably the rise of global pandemics has made governments and individuals realize the potential vulnerability. The ability to engineer biological systems are prone to risk of dual-use and could be misused to create enhanced pathogens or biological weapons.[12] The democratization of biotechnology tools and techniques makes it increasingly difficult to control who has access to these capabilities. Ensuring the security of biological research while maintaining its benefits for human health and development represents a critical challenge. Simultaneously, the development of biosecurity could be an asset internationally that should be seen as a common resource, if not the dangers of being misused was so high.

Successes and Failures in Balancing Security and Innovation: DARPA and OSINT in Ukraine

The relationship between security and innovation is complex and multifaceted, often requiring careful balance between competing priorities. Two compelling case studies—DARPA's institutional approach to fostering innovation and the role of OSINT in the Ukraine conflict – provide valuable insights into how organizations and actors navigate these challenges in practice[13]. These

[12] Benjamin D. Trump, "Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance," September 8, 2021, https://www.ncbi.nlm.nih.gov/books/NBK584259/.

[13] Swanstrom. Erixon and Guha Sarkar, T*he U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies.*

cases illustrate different aspects of the security-innovation relationship and offer lessons for future policy and practice.

DARPA: Institutionalizing Innovation in National Security

The Defense Advanced Research Projects Agency (DARPA) emerged from the Cold War need to prevent strategic technological surprise, following the Soviet Union's launch of Sputnik. Since its inception in 1958, DARPA has evolved into a unique institution that successfully bridges the gap between security requirements and innovative research.[14] Its organizational structure and operational approach offer valuable insights into how to foster innovation while serving national security objectives.

DARPA's success stems from several key organizational characteristics that enable it to balance security and innovation effectively. The agency maintains a relatively small, flat organization with rotating program managers who serve limited terms. This approach brings fresh perspectives and prevents institutional stagnation. DARPA's program managers have significant autonomy in project selection and management, allowing them to pursue promising but risky ideas that might be overlooked in more traditional research organizations.

The agency's funding model emphasizes high-risk, high-reward projects that might not find support through conventional channels. By accepting a higher failure rate than traditional research organizations, DARPA creates space for truly transformative innovations. This approach has led to breakthrough developments in areas ranging from the internet to stealth technology, demonstrating how security objectives can drive broader technological innovation.

One of DARPA's most significant contributions has been its ability to develop technologies with both military and civilian applications. The internet, GPS, and voice recognition software all emerged from DARPA-funded research. This dual-use approach helps justify investment in high-risk research while ensuring that innovations benefit both national security and econo-

[14] "About DARPA," DARPA, accessed November 19, 2024, https://www.darpa.mil/about-us/about-darpa.

mic development. It also creates pathways for technology transfer between defense and civilian sectors, maximizing the impact of research investments.

DARPA has developed sophisticated approaches to managing security concerns while maintaining the openness necessary for innovation. The agency carefully segments research projects, maintaining appropriate security controls while allowing sufficient information sharing to drive innovation. This balanced approach has enabled DARPA to work effectively with both classified defense programs and open academic research. This noted, the DARPA model should primarily be implemented among like-minded states, or even among allies in some cases.

OSINT in the Ukraine Conflict: Innovation in Real-Time Intelligence

The conflict in Ukraine has demonstrated the revolutionary potential of open-source intelligence (OSINT) in modern warfare and international security.[15] Social media platforms, commercial satellite imagery, and other publicly available data sources have created unprecedented transparency in conflict zones, fundamentally changing how information is gathered, analyzed, and disseminated.

The Ukraine conflict has spawned numerous innovations in OSINT collection and analysis. Civilian analysts and researchers have developed new techniques for verifying and correlating information from multiple sources, creating detailed pictures of military movements and operations. Social media monitoring tools, geolocation techniques, and collaborative analysis platforms have evolved rapidly in response to the conflict's demands.[16]

The proliferation of OSINT capabilities has challenged traditional approaches to operational security. Military operations that once could be conducted with relative secrecy are now visible to anyone with internet access

[15] Robin Kemp, "OSINT's influence on the Russian air campaign in Ukraine and the implications for future western deployments," *Atlantic Council*, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/osints-influence-on-the-russian-air-campaign-in-ukraine-and-the-implications-for-future-western-deployments/.

[16] Owen Vandersmith, "How Open-Source Intelligence Is Changing Warfare," *US Naval Institute*, March 2023, https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare.

and basic analytical skills. This transparency has forced military planners to adapt their approaches to operational security while also creating new opportunities for strategic communication and information operations.

OSINT has democratized access to intelligence information, allowing non -state actors, including journalists, researchers, and civilian analysts, to conduct sophisticated intelligence analysis.[17] This development has profound implications for international security, creating new channels for verification of claims and counter-propaganda, while also raising concerns about the potential misuse of sensitive information.

The widespread availability of OSINT capabilities has created new security challenges. Military forces must now operate under constant surveillance from civilian observers, requiring new approaches to operational security. The risk of disinformation and manipulation of open-source information has also emerged as a significant concern, requiring careful verification and analysis procedures.

Lessons Learned

Both cases demonstrate the importance of institutional frameworks in managing the security-innovation relationship. DARPA's structured approach to fostering innovation while maintaining security controls offers lessons for other organizations seeking to balance these competing demands. The OSINT community's development of collaborative verification and analysis methods shows how informal institutions can emerge to address new security challenges.

Both DARPA and the OSINT community in Ukraine demonstrate the importance of adaptability in responding to technological change. DARPA's rotating leadership and focus on emerging technologies help it stay ahead of technological trends, while the OSINT community's rapid development of new analytical techniques shows how innovation can occur in response to immediate operational needs.

[17] H.I. Sutton, "Reflecting on One Year of War: The Power of Open-Source Intelligence," *Center for Maritime Strategy*, February 6, 2023, https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-the-power-of-open-source-intelligence/.

Both cases also highlight the challenges and opportunities in managing information flows in security contexts. DARPA's segmented approach to research security and the OSINT community's development of verification procedures offer different models for balancing openness with security requirements.

These case studies demonstrate that the relationship between security and innovation is not simply antagonistic but can be managed productively through appropriate institutional frameworks and operational practices. DARPA's success in fostering breakthrough innovations while serving national security needs shows how organizational design can help balance competing priorities. The evolution of OSINT in the Ukraine conflict illustrates how technological innovation can transform security practices while creating new challenges that require innovative solutions.

The lessons from these cases suggest that successful management of the security-innovation relationship requires:

- Flexible institutional frameworks that can adapt to changing circumstances.
- Clear processes for managing information and security requirements.
- Support for experimentation and acceptance of calculated risks.
- Recognition of the potential for dual-use applications of new technologies.
- Continuous adaptation to evolving technological capabilities and security challenges.

Key Considerations for Policymakers

To ensure an effective balance between security and innovation, policymakers should consider:

1. Adaptive and Risk-Based Regulatory Frameworks

Policymakers should implement flexible and adaptive regulatory approaches that can evolve alongside rapid technological advancements. A risk-based framework is essential, prioritizing security measures according to the potential risks associated with specific technologies or sectors. This helps ensure that regulations remain relevant and effective without stifling innovation.

2. Regulatory Sandboxes and Dual-Use Technology Safeguards
Regulatory sandboxes allow for the testing of innovative technologies in a controlled environment under regulatory supervision. In parallel, safeguarding policies for dual-use technologies (those with both civilian and military applications) are vital. These policies should ensure that while the benefits for civilian use are promoted, the risks of misuse for military or harmful purposes are minimized.

3. Strengthening Intellectual Property Laws and Cybersecurity
Strengthening intellectual property (IP) laws and enforcement mechanisms is crucial for protecting research from theft or exploitation by hostile foreign entities. This includes fostering closer collaboration between the government and private sector to secure technological innovations, especially in high-risk sectors such as AI, cybersecurity, and biotechnology.

4. Investment in Quantum Computing and Digital Security Research
Governments should prioritize investment in quantum computing research, particularly in the development of quantum-resistant cryptography. These efforts will fortify current and future digital infrastructure, helping safeguard critical systems from potential threats posed by quantum computing capabilities in adversarial hands.

5. Education and Workforce Development in High-Risk Sectors
To maintain a competitive edge, policymakers should focus on incentivizing education and workforce development, particularly in high-risk sectors such as AI, biotechnology, and cybersecurity. Encouraging both public and private sector investment in skills training and education ensures a robust workforce ready to meet the challenges posed by rapidly evolving technologies.

Bibliography

Aghion, Philippe, Antonin Bergeaud and John Van Reenen. "The Impact of Regulation on Innovation." *Cato Institute*, April 19, 2023. https://www.cato.org/research-briefs-economic-policy/impact-regulation-innovation.

CISA, NSA, FBI, NCSC-UK, ACSC, CCCS and NCSC-NZ. "Cybersecurity Best Practices for Smart Cities." April 19, 2023. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

Corrigan, Jack, Melissa Flagg and Dewey Murdick. "The Policy Playbook." *Center for Security and Emerging Technology* (2023): 8–9. https://doi.org/10.51593/20230018.

"About DARPA." DARPA accessed November 19, 2024, https://www.darpa.mil/about-us/about-darpa.

Deloitte. "Quantum computers and the Bitcoin blockchain." *Deloitte Netherlands: Risk Advisory Perspectives*, 2023. https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.

Forbes Technology Council. "Benefits And Cautions Of Aligning With Cybersecurity Frameworks." *Forbes*, February 13, 2024. https://www.forbes.com/councils/forbestechcouncil/2024/02/13/benefits-and-cautions-of-aligning-with-cybersecurity-frameworks/.

ISACA. "Quantifying information risk and security." *ISACA Journal*, July 1, 2013. https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security.

Kemp, Robin. "OSINT's influence on the Russian air campaign in Ukraine and the implications for future western deployments." *Atlantic Council*, August 30, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/osints-influence-on-the-russian-air-campaign-in-ukraine-and-the-implications-for-future-western-deployments/.

McKinsey & Company. "A Playbook for Innovation Hubs and Ecosystems." *Global Institute for Innovation and Development*, February 28, 2023. https://giid.org/app/uploads/2024/03/A-playbook-for-innovation-hubs-and-ecosystems-McKinsey.pdf.

Swanstrom, Niklas, Fredrik Erixon and Mrittika Guha Sarkar. *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies*, Armin Lear Press, 2024.

Sutton, H. I. “Reflecting on One Year of War: The Power of Open-Source Intelligence.” *Center for Maritime Strategy*, February 6, 2023. https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-the-power-of-open-source-intelligence/.

Trump, Benjamin, D. “Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance.” September 8, 2021. https://www.ncbi.nlm.nih.gov/books/NBK584259/.

OECD. “Assessing potential future artificial intelligence risks, benefits and policy imperatives.” *OECD Artificial Intelligence Papers*, no. 27 (2024): 19–25. https://doi.org/10.1787/3f4e3dfb-en.

Vandersmith, Owen. “How Open-Source Intelligence Is Changing Warfare.” *US Naval Institute*, March 2023. https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare.

Wheeler, Tom and David Simpson. “The digital future requires making 5G secure.” *Brookings Institution*, December 12, 2022. https://www.brookings.edu/articles/the-digital-future-requires-making-5g-secure/.

https://doi org/10 59862/k7m2x9q4r8/02

Chapter 2

Academic Espionage: Finding a Better Balance between Open Science and Security Imperatives

ARTUR GRUSZCZAK
Jagiellonian University
ORCID: 0000-0002-3450-8377

Abstract: Academia has increasingly become a battleground where high-value knowledge and intellectual property are contested by public and private actors employing diverse strategies to secure or appropriate these assets for their own benefit. Universities, as centers of knowledge production, are natural targets for surveillance, recruitment, and collaboration by intelligence services. Security institutions, particularly intelligence and counterintelligence agencies, play a pivotal role in protecting the sources, repositories, and integrity of critical information and data. This chapter offers a set of recommendations addressing the challenge of safeguarding academia's principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services.

Keywords: academia; security; espionage; intelligence; counterintelligence

Research and education have long been vulnerable to malicious and disruptive activities perpetrated by various entities, ranging from populist politicians to cybercriminals. As hubs for knowledge production, professional development, and critical inquiry, these sectors face distinct vulnerabilities that can be mitigated through awareness-raising initiatives and robust risk management strategies. Among these challenges is the issue of academic espionage, which exploits the principles of open science while leveraging actionable intelligence and conventional spying techniques employed by state and non-state actors. This short analysis examines academia as a contested space where espionage and intelligence gathering undermine academic freedom and contribute to the securitization of academia.

The ideal university has traditionally been envisioned as an open, safe, and intellectually vibrant environment where students and faculty pursue a shared passion for investigating and understanding the complexities of the world. Students invest their time and energy in acquiring knowledge and skills for their future careers, while professors contribute specialized expertise and knowledge developed through rigorous research, often leading to groundbreaking discoveries, innovative technologies, and novel theoretical frameworks.

The principles and practices of open science, endorsed by UNESCO and implemented by organizations such as the European Union, reflect the interconnected nature of the contemporary world. Global cooperation and knowledge sharing are deemed essential for addressing complex social, environmental, and economic challenges. While scientific progress remains concentrated in the Global North, emerging powers such as China and India are increasingly participating in collaborative scientific endeavors. These efforts underscore the importance of initiatives promoting open science and FAIR (Findable, Accessible, Interoperable, and Reusable) data.[1]

However, science is not only a civilizational asset but also a high-value commodity with significant economic and strategic implications. Governments and private enterprises, which finance research directly or through granting agencies and foundations, have a vested interest in securing priority access to original research findings—especially those with disruptive potential for the economy, security, and society. Governments aim to ensure sustainable development, safeguard public infrastructure, and mitigate emerging risks, while businesses seek competitive advantages and market innovation. Consequently, academia has increasingly become a battleground where high -value knowledge and intellectual property are contested by public and private actors employing diverse strategies to secure or appropriate these assets

[1] UNESCO, "An introduction to the UNESCO Recommendation on Open Science," Canadian Commission for UNESCO, (2022), https://doi.org/10.54677/XOIR1696; European Commission, "Open Science," European Commission, 2024, https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en.

for their own benefit. This dynamic is particularly pronounced when such knowledge is safeguarded by patents, copyrights, or trademarks, or when it holds ethical, political, or ideological sensitivities. When the vital interests of a state—its society, economy, or national security—are at stake, security institutions, particularly intelligence and counterintelligence agencies, play a pivotal role in protecting the sources, repositories, and integrity of critical information and data. Universities, as centers of knowledge production, are natural targets for surveillance, recruitment, and collaboration by intelligence services. These institutions increasingly navigate a complex relationship with intelligence agencies, framed by shared interests in research, professionalization, and national security.

Intelligence institutions have actively sought to establish and deepen collaboration with academia for purposes such as recruitment, professionalization, and networking. Academia, in turn, has recognized several benefits of such cooperation, including professional development (e.g., incorporating former intelligence practitioners into faculty roles), enhanced research quality (through contributions by active and former intelligence professionals), and enriched scholarly output (such as intelligence-focused studies, publications, and research projects). This pragmatic engagement is conceptualized by Liam Francis Gearon through his model of the "university-security-intelligence nexus," which operates across four intersecting domains: operational, epistemological, ethical, and existential.[2] In the operational domain, Gearon highlights the practical rules governing collaboration between intelligence agencies and academia, including cases of covert partnerships and mutual support. The epistemological domain frames this nexus as an epistemic community uniting scholars and intelligence practitioners to generate knowledge and expertise aimed at countering security threats. The ethical domain addresses questions of moral responsibility and the ethical implications of intelligence and security influence within academic institutions. Lastly, the existential domain situates this nexus within the broader context

[2] Liam Francis Gearon, "The University-Security-Intelligence Nexus: Four Domains," in The Routledge International Handbook of Universities, Security and Intelligence Studies, ed. Liam Francis Gearon (London: Routledge, 2020), 15.

of pressing national security threats, societal risks, and individual vulnerabilities, emphasizing its role in mitigating complex contemporary challenges. Gearon argues that this model signifies a shift in intelligence and security paradigms, from traditional, narrowly focused frameworks to more expansive, integrated approaches that harness academic insights and intelligence expertise to mitigate evolving threats.[3]

Similarly, Vogel et al.[4] examine Academic–Industry–Intelligence Collaboration through the lens of initiatives like the US National Security Agency's (NSA) establishment of the Laboratory for Analytic Sciences (LAS). They contend that institutions such as the NSA can drive organizational innovation and adaptation by fostering inter-institutional and interdisciplinary collaboration between academics and intelligence professionals, yielding mutually beneficial outcomes for both domains.

Despite potential synergies, the entanglement between academia and intelligence often results in blurred boundaries and hidden agendas, which can undermine the core academic values of openness, freedom, and objectivity. These dynamics manifest in three key areas:

1. Exploitation of Research Outputs

Advanced research, particularly in critical fields such as defense and technology, is a prime target for espionage. For example, concerns over Chinese espionage in US universities have highlighted vulnerabilities, such as unauthorized knowledge transfer and cyber intrusions.[5] Initiatives such as China's Thousand Talents Program (TTP) have fueled geopolitical tensions, prompting countermeasures like the US Department of Justice's "China

[3] Ibid, 14–15. See also: Stéphane Lefebvre, "Academic-Intelligence Relationships: Opportunities, Strengths, Weaknesses and Threats," Journal of Policing, Intelligence and Counter Terrorism 16, no. 2 (2021), https://doi.org/10.1080/18335330.2021.1880020.

[4] Kathleen M. Vogel et al., "The Importance of Organizational Innovation and Adaptation in Building Academic-Industry-Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences," The International Journal of Intelligence, Security, and Public Affairs 19, no. 3 (2017), https://doi.org/10.1080/23800992.2017.1384676.

[5] Larry Diamond and Orville Schell, eds. China's Influence & American Interests: Promoting Constructive Vigilance. Report of the Working Group on Chinese Influence Activities in the United States, rev. ed. (Stanford, CA: Hoover Institution Press, 2019).

Initiative."[6] While the scale of Chinese espionage may be overstated, similar concerns have been raised by the governments of the UK, Germany, and Australia, emphasizing the risks posed by adversarial actors.

Elizabeth A. Rowe, a Professor of Law at the University of Virginia School of Law, investigated cases of academic espionage and compiled a list of eleven Chinese "professors in handcuffs." She interpreted these cases as evidence of a disconnect between the individual criminal liability of academic staff and the distributed accountability of universities as legal entities.[7] Despite controversies surrounding the measures adopted by the US authorities, reports detailing extensive espionage efforts to circumvent research security protocols and exploit the principles of open science for adversarial purposes have also been released by the governments of the UK, Germany, and Australia. While these reports primarily focus on China's operations, they also underscore escalating espionage activities by Russia, particularly after 2022.[8]

2. Personal Ties Between Academia and Intelligence

Scholars can become associated with intelligence institutions in various ways. From the perspective of national intelligence services in a scholar's country of residence, their knowledge, expertise, experience, and exceptional intellectual capabilities are regarded as particularly valuable resources. Scholars are often approached for cooperation, typically in an advisory capacity, to help intelligence services refine their intelligence cycle and enhance analytical capabilities. For example, media reports have highlighted that distinguished American academics such as Robert Jervis, Joseph S. Nye, and H. Bradford Westerfield served as advisors to the CIA.[9] A specific

[6] Kathleen M. Vogel and Sonia Ben Ouagrham-Gormley, "Scientists as Spies? Assessing U.S. Claims about the Security Threat Posed by China's Thousand Talents Program for the U.S. Life Sciences," Politics and the Life Sciences 42, no. 1 (2023), https://doi.org/10.1017/pls.2022.13.

[7] Eileen Guo, Jess Aloe, and Karen Hao, "The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It," MIT Technology Review, December 2, 2021, https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

[8] Alexander Martin, "British Intelligence Moves to Protect Research Universities from Espionage," The Record, April 26, 2024, https://therecord.media/MI5-protect-british-universities-from-espionage.

[9] David N. Gibbs, "Academics and Spies: The Silence That Roars," Los Angeles Times, January 28, 2001, https://irp.fas.org/news/2001/01/lat012801.html.

pattern has emerged in the field of intelligence studies, where former intelligence officials are hired as faculty members. They bring practical knowledge and firsthand experience, enriching academic discourse and contributing to the professional education of future intelligence personnel. From a counterintelligence perspective, academia is a significant target for espionage and adversarial intelligence activities by foreign services. These entities aim to identify and recruit informants among students and professors. If successful, they can gain access to restricted or sensitive research data or collect large volumes of data generated in critical fields of science and technology.

3. Future Careers

Outstanding students, top graduates, and prominent activists within student circles are often targeted as valuable assets for long-term collaboration with intelligence institutions. Domestic intelligence services employ headhunting strategies to recruit individuals with high potential as effective personnel. Conversely, adversary services deploy tactics to identify and groom potential agents of influence by offering discreet assistance—whether material or financial—facilitating career advancements or integrating them into strategically designed networks of influence. The case of Ana Montes serves as a compelling example of how academia can function as a fertile environment for recruitment.[10]

It is overly optimistic to regard academia as a "neutral ground" where the noble pursuit of science is achieved through the objective search for truth. The collegial academic environment, characterized by a spirit of freedom, openness, and the unrestricted exchange of ideas, has long been a hallmark of academia's role in a complex and interconnected world. Features such as unrestricted access to university facilities, open admissions to conferences, seminars, and public lectures, minimal security screening of students enrol-

[10] Ana Belen Montes was a graduate student at the Johns Hopkins University where she was recruited in 1984 by a fellow student to collaborate with the Cuban Intelligence Directorate (G2). Under guidance from G2 officers, she was employed as an intelligence analyst at the Defense Intelligence Agency (DIA) and later became its most senior Cuban analyst.

ling in programs, and tolerance for unconventional or unorthodox behaviors displayed by students or faculty have traditionally been seen as valuable and integral to academic culture.

However, as Anthony Bishop—an academic and former CIA officer—notes, these very attributes create "the perfect opportunity for undercover foreign intelligence officers or their human sources to slip onto campus and search for students who have potential for entering sensitive positions in the US. government or landing jobs with American companies engaged in the development and production of emerging and advanced technologies."[11] Elisabeth A. Rowe underscores that "academia is grounded not in a culture of ownership and secrecy, but of openness and sharing."[12] Yet, this culture—geared towards disseminating research outcomes through papers, articles, books, speeches, seminars, and conferences—renders academia "a valuable, vulnerable, and low-risk target for foreign espionage."[13] While open science promotes greater accessibility, inclusivity, and transparency, advancing the right of all individuals to share in scientific progress and its benefits, it does not adequately address the challenges of safeguarding scientific achievements against unlawful or malicious exploitation by academic and non-academic actors alike.

Recommendations

The challenge of safeguarding academia's principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services, can be addressed through the following recommendations:

Awareness raising through training courses for faculty and administrative staff

Both basic and advanced training courses should be implemented to heighten awareness of the risks and vulnerabilities that make academia a target

[11] Anthony Bishop, "International Espionage on Campus," The World Deciphered, November 6, 2016, https://www.thecipherbrief.com/column_article/international-espionage-on-campus.

[12] Elizabeth A. Rowe, "Academic Economic Espionage?" William & Mary Law Review 65, no. 1 (2023), 7, https://scholarship.law.wm.edu/wmlr/vol65/iss1/2.

[13] Daniel Golden, Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities (New York: Henry Holt & Co., 2017), 23.

for espionage. Such courses can be designed and delivered systematically by intelligence professionals in collaboration with university authorities.

Resilience building through security preparedness for sensitive research and educational programs

Scholars engaged in sensitive and high-stakes research should receive proper guidance on the risks posed by foreign intelligence services. They must also be held accountable for ensuring that the outcomes of their research are handled responsibly and securely.

Ethics and diligence in open science (addressing the AI dilemma)

The growing reliance on AI-driven research necessitates the establishment of robust regulations and standards to ensure full adherence to ethical principles and due diligence. These measures will mitigate risks without stifling innovation.

Stricter knowledge management and intellectual property protection

Security vetting of key research projects should become standard practice to prevent unauthorized or illicit access to sensitive findings. Universities must cultivate a culture of proprietary awareness and establish systematic infrastructures for safeguarding intellectual property. While these measures do not undermine the principle of open science, they promote a more prudent approach to managing research outcomes and translating them into practical applications.

A more targeted visa policy

Universities, in coordination with relevant authorities, should implement a more nuanced approach to long-term visa issuance. While protecting individuals' rights to study and reside (including students and faculty), visa processes can serve as an initial screening mechanism to reduce the risk of infiltration by individuals potentially involved in espionage.

Effective and balanced cooperation with state security and counterintelligence agencies

Elizabeth A. Rowe described the academic sphere as a site of "collision between espionage, secrecy, national security, criminal law, and the academic environment."[14] This contrasts with Liam Francis Gearon's symbiotic perspective, highlighting divergent views on academia's role within the interplay of government, security services, the judiciary, private enterprise, and civil society. Despite academia's discomfort with such entanglements, the growing scale and diversity of espionage activities targeting universities require decisive, precautionary measures. These actions should involve close collaboration between university authorities and state security agencies.

A Necessary Disclaimer

The above recommendations apply to academic environments where the principles of open science serve as the foundation for education and research. They are not intended for authoritarian systems, where ideological agendas and political objectives often suppress academic freedom. In such regimes, partnerships between academia and intelligence services are typically government-mandated, aiming to place universities and research institutions under strict control and surveillance. Under these conditions, academia often becomes a tool of the state, unable to fulfill its mission of advancing truly open science.

The challenge of safeguarding academia's principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services, can be addressed through the following recommendations:

- Awareness raising through training courses for faculty and administrative staff.
- Resilience building through security preparedness for sensitive research and educational programs.
- Ethics and diligence in open science (addressing the AI dilemma).
- Stricter knowledge management and intellectual property protection.

[14] Elizabeth A. Rowe, "Academic Economic Espionage?" William & Mary Law Review 65, no. 1 (2023), 76, https://scholarship.law.wm.edu/wmlr/vol65/iss1/2.

- A more targeted visa policy.
- Effective and balanced cooperation with state security and counterintelligence agencies.

Bibliography

UNESCO. *"An introduction to the UNESCO Recommendation on Open Science." Canadian Commission for UNESCO*, 2022. https://doi.org/10.54677/XOIR1696.

Bishop, Anthony. *"International Espionage on Campus." The World Deciphered*, November 6, 2016. https://www.thecipherbrief.com/column_article/international-espionage-on-campus.

Diamond, Larry and Orville Schell, eds. *China's Influence & American Interests: Promoting Constructive Vigilance. Report of the Working Group on Chinese Influence Activities in the United States*, rev. ed. Stanford: Hoover Institution Press, 2019.

Gearon, Liam Francis. "The University-Security-Intelligence Nexus: Four Domains." In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, edited by Liam Francis Gearon. Routledge, 2020, 15.

Gibbs, David N. "Academics and Spies: The Silence That Roars." *Los Angeles Times*, January 28, 2001. https://irp.fas.org/news/2001/01/lat012801.html.

Golden, Daniel. *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*. New York: Henry Holt & Co., 2017.

Guo, Eileen, Jess Aloe and Karen Hao. "The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It." *MIT Technology Review*, December 2, 2021. https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

Lefebvre, Stéphane. "Academic-Intelligence Relationships: Opportunities, Strengths, Weaknesses and Threats." *Journal of Policing, Intelligence and Counter Terrorism* 16, no. 2 (2021). https://doi.org/10.1080/18335330.2021.1880020.

Martin, Alexander. "British Intelligence Moves to Protect Research Universities from Espionage." *The Record*, April 26, 2024. https://therecord.media/MI-5-protect-british-universities-from-espionage.

European Commission. "Open Science." *European Commission*, 2024. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en.

Rowe, Elizabeth A. "Academic Economic Espionage?" *William & Mary Law Review* 65, no. 1 (2023). https://scholarship.law.wm.edu/wmlr/vol65/iss1/2.

Vogel, Kathleen M., and Sonia Ben Ouagrham-Gormley. "Scientists as Spies? Assessing U.S. Claims about the Security Threat Posed by China's Thousand Talents Program for the U.S. Life Sciences." *Politics and the Life Sciences* 42, no. 1 (2023): 32–64. https://doi.org/10.1017/pls.2022.13.

Vogel, Kathleen M., et al. "The Importance of Organizational Innovation and Adaptation in Building Academic-Industry-Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences." *The International Journal of Intelligence, Security, and Public Affairs* 19, no. 3 (2017). https://doi.org/10.1080/23800992.2017.1384676.

https://doi org/10 59862/k7m2x9q4r8/03

Chapter 3

Cybersecurity in the Academic Environment: Scientific Institutions as Targets of Cyber-attacks

ANDRII DAVYDIUK
G.E. Pukhov Institute for Modelling in Energy Engineering
at National Academy of Sciences of Ukraine
ORCID 0000-0003-1238-2598

Abstract: Scientific institutions and research facilities are increasingly becoming targets of cyberattacks. The consequences of such attacks can include data theft and integrity breaches, loss of intellectual property, reputational damage, and threats to national security. This study proposes to examine scientific institutions as multi-layered targets for malicious actors who may have espionage and destructive motives. Key sub-targets that are frequently attacked include students, faculty, other staff, databases, neural network-based systems and artificial intelligence, as well as other IT systems. This approach allows for the formation of a structured cybersecurity profile of the research institution. By "profile," proposed to mean a set of typical characteristics of scientific institutions in the context of cybersecurity. This research aims to develop a cybersecurity profile for scientific institutions that includes a classification of typical threats, a list of potential attack targets, and possible risks. A separate analysis of case studies based on real examples is also conducted. This profile will not only help identify the main vulnerabilities of the institution but will also serve as a practical tool for enhancing cybersecurity within the academic environment. Specifically, this section attempts to summarize knowledge about cyber threats in the academic sector and propose concrete methods for protecting critical data and research resources.

The relevance of this research is confirmed by real threats, including espionage by China against the United States and other countries.[1] Moreover, the involvement of scientific institutions as subjects of cyberattacks2 also represents a distinct threat in cyberspace, which will have a unique profile. A striking example of the importance of cybersecurity in the scientific sector is the war in Ukraine, where scientific institutions are actively targeted by adversaries. Data about research projects in the fields of security and defense, energy, etc., as well as personnel lists of military institutes, are valuable to adversaries. Such information allows for the assessment of the strength and capabilities of the Ukrainian army and is used to prepare battle strategies. This underscores the strategic significance of information and cybersecurity for scientific institutions in military conflicts. The proposed profile can be used to develop effective cybersecurity measures aimed at protecting critical data and reducing risks in the academic environment. At the same time, it also promotes collaboration between scientific institutions and governmental bodies in the field of cybersecurity for data and protection method exchange, including in an international context. This approach is particularly relevant for countries experiencing military conflicts or facing intense cyber threats from foreign states.

Keywords: cyberattacks, cybersecurity, scientific institutions, intellectual property, national security

Scientific and educational institutions are an important component of the state. The training of specialists, conducting research, attracting foreign investments depends on them. Ensuring cyber security and information security is an integral part of the functioning of any scientific institution. Vulnerabilities in the education sector go far beyond immediate disruption, but can potentially compromise research integrity, data privacy, and the financial stability of these outstanding institutions.

Let's consider in more detail why scientific institutions become the targets of cyber-attacks. One of the reasons may be an offended student who, in his or her opinion, received a low grade and wants to take revenge on the educa-

[1] "Survey of Chinese Espionage in the United States Since 2000," Center for Strategic and International Studies, accessed November 21, 2024, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

[2] Dakota Cary, "Academics, AI, and APTs," Center for Security and Emerging Technology, March 2021, https://cset.georgetown.edu/publication/academics-ai-and-apts/.

tional institution. Another motive on the part of the student may be to sabotage the educational process due to unwillingness to pass the test or change the assessment results. However, it is not only students that pose a threat. An educational institution can become a victim of a cyber-attack due to unfair competition. Obtaining grants is always a competition and reputational damage due to missed deadlines can be the reason for refusal of grants. One cannot reject the natural competition among scientists for the primacy of discovery and scientific glory. All these factors can be attributed to internal threats, but in addition, there are also external ones.

External threats include primarily espionage, theft of ideas, and slowing down of research. A vivid example of such a hunt for information was the Cold War.[3] Another example is attacks on scientific institutions conducting COVID-19 research that were a significant cyber threat during the pandemic. Hacker groups such as APT29 (linked to Russia) have attempted to steal information related to the development of vaccines against COVID-19. The attackers used special malware ("WellMess" and "WellMail") as well as known software vulnerabilities to gain access to the networks of institutions in Canada, the United States and the United Kingdom.[4] [5] During the Russian-Ukrainian war, the object of the enemy's interest, among others, are military educational institutions that prepare future officers for the Ministry of Defence, the armed forces, and other military formations. For the enemy, they are a source of data on the number of specialists, their level of training, material base, individual cadets and officers who can be swayed to their side. All these data enable the enemy to more effectively prepare for war and develop attack tactics. In addition, departmental institutes of the defense sector can be exposed to cyber-attacks as

[3] John L. Gaddis, "Intelligence, Espionage, and Cold War Origins," Diplomatic History 13, no. 2 (1989), 191–212.

[4] Cybersecurity and Infrastructure Security Agency, "COVID-19 Cyber Threats (Update)", August 30, 2020, https://www.cisa.gov/sites/default/files/publications/202008131030_COVID-19%20Cyber%20Threats%20Update_TLP_WHITE.pdf.

[5] Adam Bannister, "Bad Education: Universities Struggle to Defend Against Surging Cyber-Attacks During the Coronavirus Pandemic," The Daily Swig | Cybersecurity News and Views, February 23, 2021, https://portswigger.net/daily-swig/bad-education-universities-struggle-to-defend-against-surging-cyber-attacks-during-coronavirus-pandemic.

part of the department that the adversary wants to damage. For example, DDoS attacks on their websites, disruption of training processes, etc. In the spring of 2020, the number of DDoS (Distributed Denial of Service) attacks in the education sector increased by 350%.[6] The percentage increase of such attacks on the education sector in 2021 was 102%. Such attacks disrupt critical operations such as class scheduling, assignment, and the admissions process.[7] For example, the hacktivist group Anonymous Sudan launched a DDoS attack against some of the UK's top universities. This attack caused significant damage and disruption. Because of this attack, the Computing Service of the University of Cambridge Clinical School had to experience unstable internet access. Shedding light on the interconnected nature of cyber risks at universities, the network issue was just one part of a larger attack on the Jane Network. Jane's network unites several universities.[8] But there were also other types of attacks, for example, you can cite an incident at the University of Minnesota, when in 2021, cybercriminals hacked into a database containing student financial applications. The attackers gained access to personal information, including names, addresses, social security numbers and even passport information. The leak was only discovered in 2023, when the stolen data began to appear online.[9] In 2023, Indiana University was found to have stored student survey data that included sensitive information (sexual orientation, race, etc.) on unsecured cloud storage. This led to the leak of almost 250,000 records.[10]

[6] "DDoS Attacks Against Educational Resources Increased by More Than 350%, Says Kaspersky," *Intelligent CIO* https://www.intelligentcio.com/me/2020/09/15/ddos-attacks-against-educational-resources-increased-by-more-than-350-says-kaspersky/.

[7] NETSCOUT Systems, Inc., "Bad Actors Innovate, Extort and Launch 9.7M DDoS Attacks in 2021 According to the Latest NETSCOUT Threat Intelligence Report," March 22, 2022, https://ir.netscout.com/investors/press-releases/press-release-details/2022/Bad-Actors-Innovate-Extort-and-Launch-9.7M-DDoS-Attacks-in-2021-According-to-the-Latest-NETSCOUT-Threat-Intelligence-Report/default.aspx.

[8] James Coker, "Top UK Universities Recovering Following Targeted DDoS Attack," Infosecurity Magazine, February 20, 2024, https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/.

[9] University of Minnesota System, "Data Incident," University of Minnesota System, accessed November 24, 2024,https://system.umn.edu/data-incident.

[10] "IU Reports Records Exposed in Data Breach Are Public Domain," Indiana Public Media, July 13, 2023, https://indianapublicmedia.org/news/indiana-university-suffers-second-data-leak-this-year.php.

Exploitation of vulnerable file transfer software (MOVEit) allowed cybercriminals to gain access to student and employee data at the University of Georgia, including social security numbers, contact information, and payroll information.[11] Lincoln College was forced to close due to a massive ransomware attack in 2021. The attack disrupted access to data and complicated the process of recruiting students, which caused significant financial losses and became fatal for the institution.[12] In June 2022, the University of Pisa fell victim to the BlackCat ransomware group, which hijacked the university's IT system before demanding a whopping $4.5 million ransom, making it one of the largest ransom demands of 2022.[13] Cyberattacks can disrupt and disable critical systems that support student registration portals, learning systems, and financial transaction systems. This may lead to interruption of educational activities and administration work. For example, in 2023 there was a large-scale attack on "Neptune," an online portal for students and teachers used by the University of Pecs and other universities in Hungary. The attack occurred during university exams and caused serious service disruptions. The universities had to face the system failure for two months. Academic evaluations were delayed and administrative work was distracted due to the temporary shutdown of the system. The shutdown also proved that key academic systems are not immune to cyberattacks.[14]

A separate aspect of the information security of educational institutions is the physical security of their IT systems, as there have already been cases of kinetic attacks on educational institutions. Specifically, on September 3, 2024, two Russian missiles hit a branch of the Military Institute

[11] University System of Georgia, "Notice of Data Breach," University System of Georgia, April 15, 2024, https://www.usg.edu/news/release/notice_of_data_breach.

[12] Graham Cluley, "US College Set to Permanently Close After 157 Years, Following Ransomware Attack," Hot for Security, May 11, 2022, https://www.bitdefender.com/en-us/blog/hotforsecurity/us-college-set-to-permanently-close-after-157-years-following-ransomware-attack.

[13] Scott Zelko, "A Recap of Recent Cybersecurity Incidents at Universities," Schellman Compliance, November 14, 2023, https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023.

[14] Fares Barauj, "Importance of Cybersecurity in Educational Institutions," July 2024, https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions.

of Telecommunications and Information Technologies and a nearby hospital in Poltava, Ukraine, killing at least 59 and injuring at least 328.[15]

It is worth noting that the targets of cyber-attacks are not only educational institutions, but also teachers and researchers working in them. Many of the teachers take their work home and work from their own computer, so the personal device is a data carrier for research and may have access parameters to the resources of the educational institution. In addition, scientists who are teachers can hold positions in production or take part in public administration. With this in mind, cyber security in academic institutions should include protection of IT systems used for research and cyber hygiene work for staff, and cyber security in the scientific sphere becomes a matter of national security. Overall, the record growth in attacks in the third quarter of 2024 saw an average of 1,876 cyberattacks per organization, a 75% increase over the same period in 2023 and a 15% increase over the previous quarter. And the education/research sector was the most attacked with 3,828 attacks per week, followed by the government/military and healthcare sectors with 2,553 and 2,434 attacks respectively (see Figure 1).[16]

Of course, information security is also affected by the working conditions of scientists. This includes the quality of hardware and software for cyber protection, the presence of information security policies in place, the awareness of personnel about cyber security threats and their actions in the event of a cyber-attack. Unfortunately, not all educational institutions can afford expensive hardware and software to protect their own systems, provide adequate remuneration for an information security specialist, or open such a position. Because of this, many senior teachers, due to their low level of awareness in working with digital technologies, become victims of phishing, malware, extortionists, and data encryptors. The University of Arkansas is a real-life example of phishing in higher education. The university witnessed

[15] RCB-Ukraine, “Russia Strikes Educational Institution With Ballistic Missiles in Poltava: 41 Killed, 180 Wounded,” RBC-Ukraine, September 3, 2024, https://newsukraine.rbc.ua/news/russia-strikes-educational-institution-with-1725366089.html.

[16] Check Point Team, “A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide,” Check Point Research Blog, October 25, 2024, https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

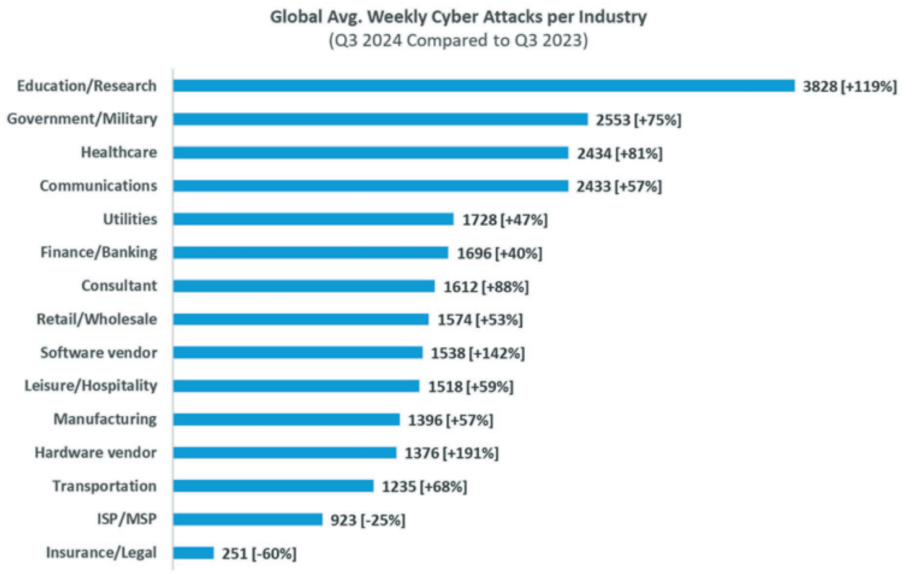

Figure 1. Comparison of the number of cyber-attacks per week by sector

a noticeable increase in the number of phishing emails. Faculty, staff, and students were the subjects of these emails. The university said the attacks resulted in many members becoming victims and accounts being compromised. The importance of being vigilant and educated about cyber security is highlighted by the rise in phishing attacks, especially during downtime. Several methods have been implemented by the University of Arkansas to overcome the dangers of this threat.[17]

The presence of such problems requires the development of a systematic approach to information protection in scientific institutions. Thus, it is expedient to classify scientific institutions. This classification may differ from general practice, in particular by subordination, specialties, etc. Classification in the field of information security is designed to identify potentially attractive scientific institutions for the enemy, and to identify critical processes, research, and possible threats in them. Appropriate measures in such a clas-

[17] Fares Barauj, "Importance of Cybersecurity in Educational Institutions," July 2024 July 2024 https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions.

sification would include dividing institutions into military and civilian categories; considering whether they conduct research in security, defense, national security, or critical infrastructure; identifying any international collaborations; and noting whether their staff includes representatives from government bodies, the security and defense sector, or related industries. Such a classification will make it possible to determine the specifics of the work of such institutions, in particular, work with information with limited access, requirements for personnel, and requirements for IT systems of such institutions. After such a basic classification, it will be possible to proceed to the prioritization of scientific institutions according to the impact of their activities on national security. By impact, it will be possible to qualitatively distinguish critical and important for national security.

At this stage, the question arises of developing requirements and evaluation methods (self-evaluation) of educational institutions of different categories in accordance with the classification proposed above. The requirements should be based on the profile of the institution according to the classification and take into account the assessment of the disruption of research processes (damage) or the leakage of sensitive research data. For example, military institutions should focus on protecting the personal data of cadets and employees, limiting access to information about the material base and the content of educational programs. The assessment (self-assessment) should include an assessment of the state of cyber protection of the IT infrastructure and the available means for this. Availability of security policies and staff awareness of cyber hygiene rules. This will enable effective planning to build their cyber security capabilities.

A separate aspect of cyber security is the possibility of the adversary using scientific institutions for cyber-attacks. Poorly protected servers, desktops in computer science classes, and clusters can be used for cyber-attacks if an attacker has unauthorized access. The use of such concentrated multi-user resources enables the attacker to increase his or her own anonymity and complicate the task of rapid localization for the defense side.

Therefore, scientific institutions need a systematic approach to cyber protection. The development and implementation of such an approach requires educational and scientific institutions to develop their own capacities and the attraction of resources. Quantum computing opens up new possibilities for attacks. Quantum computer algorithms can break modern encryption systems, putting even the most protected institutions at risk. In addition, the aggravation of geopolitical tensions at the present time increases the risks of cyberespionage, which is especially dangerous for scientific institutions with international projects. Thus, the issue of cyber security, in addition to national security, should be a matter of cyber diplomacy and diplomacy in science. At the same time, international collaboration around the problems of cyber and information security can significantly draw attention to this problem and facilitate processes in the government to develop relevant regulatory documents for the institutionalization of these processes. It is worth noting that information protection processes should not create a negative impact on the implementation of open science and the reproduction of science.

Personal

1. Use two-factor authentication.[18]
2. Remember to protect your hardware, such as setting BIOS/UEFI passwords, locking your computer when you're away, using secure workstations.
3. Use licensed/legalized operating systems and other software products, and systematically update them in a timely manner.
4. Use antivirus software with heuristic analysis technology.
5. Use a software firewall and standard anti-malware tools.
6. Back up your data regularly, store backups on external media (SSD, HDD, etc.), and set up system restore.
7. Cloud services that use synchronization (for example, Dropbox, One-Drive, SharePoint, and Google Drive) should not be used as the only environment for saving backup copies. The disadvantage of these systems is that they can automatically synchronize immediately after infection of the files, and it is also possible to lose backup copies.

[18] CERT-UA, Фактор кібербезпеки, April 1, 2024, https://cert.gov.ua/recommendation/6278274.

Note. For the most part, encrypted files cannot be decrypted by anyone. Don't waste your time or money on services that promise to do this. In some cases, cyber security experts can provide programs that can decrypt files due to malware flaws. We recommend not using programs to decrypt data from unverified sources.

8. Do not connect flash drives and external drives, do not insert CDs and DVDs, etc., into your computer unless you fully trust their source. There are techniques for hacking your computer even before you open the file on the flash drive and long before your antivirus scans it. If you found a device inside the office or on the street, received it in the mail or with a delivery, or a stranger gave it to you with a request to print a document, or simply open it and check its contents, there is a good chance that the device is dangerous.
9. Only trust your own devices and be careful with devices you receive from other people for work or other purposes.
10. When connecting devices, ensure that they are automatically checked for malware.
11. Disable automatic startup of removable media (protection from autorun.inf).
12. Do not store authentication data in easily accessible places (for example, on the desktop). Use special software tools (for example, KeePass) to store passwords. Use strong passwords, in particular, those that: contain at least eight characters; contain letters, numbers and special characters; do not contain personalized information (date of birth, phone numbers, numbers and series of documents, vehicles, bank card, registration address, etc.); not used in any other accounts.
13. Avoid using internet banking, electronic payment systems, entering authentication data when accessing the internet through public (unsecured) wireless networks (in cafes, bars, airports, and other public places).
14. Be especially careful when opening email attachments from unknown persons. Today, the most relevant means of distributing malware is email. When working with email, you should check the extensions of attached files and not open files even with safe extensions. Do not follow

unknown links or download files with potentially dangerous extensions (e.g.: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js, etc.) and even safe ones (e.g.: .docx, .zip, .pdf), because vulnerabilities, macros, and other dangers may be used. Pay attention to the email name: even if it seems legitimate, you still need to verify (by phone or otherwise) that the person actually sent you the message with the attachment.

15. Sometimes, especially under time pressure, it can be difficult to distinguish malicious files from legitimate files. Use the service VirusTotal[19] to check suspicious files by simultaneously scanning them with more than 50 antiviruses. This is much more efficient than scanning files with an antivirus offline, but consider the fact that by uploading files to VirusTotal, you are giving access to it to a third party. We draw your attention to the fact that even if the check on VirusTotal did not give a result, this does not exclude the fact that the file may be malicious.
16. Think twice before opening attachments.
17. When using internet resources (internet banking, social networks, messaging systems, news, online games), do not open suspicious links (URLs), especially those that point to websites that you do not normally visit.
18. Be alert to internet scams. The most common means of deception on the internet is phishing. Pay special attention to the domain name of the internet resource that asks for authentication data before clicking on the link: attackers can mask the domain name to make it look familiar (facelook.com, gooogle.com, etc.). Otherwise, there is a high probability of going to a phishing page, which is identical to the real one, and "giving away" your own authentication data.
19. If you need to enter credentials, make sure you're using a secure HTTPS connection, and check the website's SSL certificate to make sure it hasn't been cloned or spoofed.
20. Malicious URLs can be encoded in the form of QR codes and/or printed on paper, including in the form of shortened URLs generated by

[19] VirusTotal, https://www.virustotal.com/gui/home/upload.

special services such as tinyurl.com, bit.ly, ow.ly, etc. Do not enter these links into a browser or scan QR codes with your smartphone if you are not sure of their content and origin.

21. Use VirusTotal[20] to check for suspicious links in the same way as for scanning files.
22. Be careful about pop-ups and messages in your browser, apps, operating system, and mobile device. Always read the contents of these windows and do not "approve" or "accept" anything hastily.
23. When using remote access, it is necessary to limit access using "white list" (IP whitelisting).
24. Set a limit on the number of incorrect logins/passwords. Regularly review the login logs, task scheduler, and autostart for unauthorized activity.
25. Stay up-to-date on new cyber threats and respond quickly to new challenges.[21]

For Institutions

1. Advise employees to conduct a potential risk assessment, such as studying possible attack scenarios that may target their institution or position.
2. Conduct training for employees on protection against social engineering methods (in particular, telephone attacks, blackmail, manipulation).
3. Emphasize the importance of paying attention to unusual events—for example, sudden changes in settings, the appearance of unusual programs or files.
4. Ensure availability of system administrators (security administrators) at the object(s).
5. Ensure monitoring of information security events.
6. Identify responsible persons for responding to cyber incidents during interaction with relevant government agencies.

[20] VirusTotal, https://www.virustotal.com/gui/home/upload.

[21] CERT-UA, Основні правила кібергігієни, December 13, 2018, https://cert.gov.ua/recommendation/31.

7. Form a team of IT (information security) specialists to respond to computer emergency events.
8. Create an incident response plan, including attack recovery scenarios, and train employees on what to do in such situations.
9. Regularly audit all devices, software, and access to ensure you are in control of your infrastructure.
10. Conduct training with all employees who have access to information systems on compliance with information security policies (cyber hygiene rules) and pay attention to the use of internet resources and email, responding to phishing messages.
11. Back up critical (important) information resources and store their backup copies in separate data repositories.
12. Update operating systems and software to the latest versions.
13. Enable all possible event logging options and ensure their storage on a separate disk storage.
14. Check and enable anti-virus protection and update the anti-virus software signature database.
15. Create policies that will only allow downloading files of the types that should be received (for example, prohibit receiving or transferring .EXE files).
16. Block websites that are harmful.
17. Check suspicious files by antivirus programs, in the absence of a licensed antivirus, we recommend using the free VirusTotal or Cuckoo sandbox service.
18. If this is relevant for the institution (for example, in the case of public services), implement a solution to prevent DDoS attacks.
19. Use signatures to block known malicious code.
20. Use mail filtering (combined with spam filtering) that can block malicious email messages and delete suspicious attachments.
21. Use tools that block known malicious websites on relevant lists.
22. Use tools with information security features that can scan data content for known malware.

23. When using remote access, only allow connection to specified users using “white list” (IP whitelisting).[22]
24. For internal information exchange, it is recommended to use solutions with end-to-end encryption.
25. Carry out self-scanning for vulnerabilities of information resources posted on the internet or contact the relevant state body.
26. Eliminate vulnerabilities in information systems.
27. Disable remote access to information systems or review the circle of employees who are granted the right to remote access to information systems during the holidays, and implement maximum restrictions (filtering by IR, protocols, access time, users, etc.).
28. Implement the principle of least privilege (Least Privilege) for all employees and systems.
29. Provide security policies for employees’ mobile devices (e.g., data encryption, mandatory use of passwords, ability to remotely delete data).
30. If the institution uses the API, configure protection against unauthorized access, for example, using OAuth 2.0 or other modern standards.
31. It is also recommended to add a separate section to protect IoT devices (if used) and avoid using equipment that does not support regular firmware updates.
32. Only use securely protected remote access methods and protocols for the administration of information systems and resources that have an appropriate level of encryption.
33. Use strong passwords and set up multi-factor authentication.[23]
34. Block access from the internet to versions of software and information systems that are no longer supported by the manufacturer or the functioning of which is not critical.
35. Turn off all services and information systems that will not be used.[24]

[22] CERT-UA, Зага++льні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення, July 21, 2020, https://cert.gov.ua/recommendation/2502.

[23] National Cyber Security Centre, Top Tips for Staying Secure Online, December 21, 2021, https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers.

[24] SCPC-UA, Recommendations from the State Cyber Protection Center, January 24, 2022, https://scpc.gov.ua/uk/recommendations/129.

36. Constantly monitor the versions of the operating system, content management system (CMS), package manager, frameworks or other software that ensure the operation of the web resource, and regularly update them. At the same time, it is better to use only the "LTS" version.
37. The use of the HTTPS protocol guarantees the integrity and confidentiality of interaction with the server and protects user data when transmitted over the internet. The certificate must be issued by a certification authority.
38. Use the latest version of TLS (SSL has flaws and vulnerabilities and is not acceptable for secure communication).
39. It is a good practice to configure the HSTS (HTTP Strict Transport Security) mechanism to force HTTPS to be used, even when clicking on links that explicitly specify the HTTP protocol.
40. If the web resource does not have its own logging system, monitor the log files of the web server (access.log). In the log files, pay attention to POST requests and the server's response code to them.
41. Pay special attention to POST requests to pages that should not receive any data, or that should not exist at all. This may indicate unauthorized actions with the web resource.
42. Usually, after hacking web resources, attackers leave backdoors (webshells) on the server for remote access to the site's server. Periodically check the web application directories for such backdoors. For this purpose, it is possible to use special scripts or simply check the presence of new files in the directories. The detection of files created by third parties will indicate the hacking of the web resource and provide opportunities for further actions to find vulnerabilities that were used.[25]
43. Configure file and directory permissions. Distribute access rights to files on the server and individual sections of the site according to user tasks. Distinguish between the location of scripts and programs, data intended for reading only, and data intended for modification by visitors.

[25] CERT-UA, Рекомендації з самостійного пошуку та ліквідації веб-шеллів, https://cert.gov.ua/files/pdf/CUA-14-06R.pdf.

44. Hacking a website starts with gathering information about the server. Hiding versions of the used software is one of the elements of ensuring the security of the web server. Knowing the versions of these programs can facilitate the attacker's task of finding vulnerabilities known for this version and, as a result, in achieving the main goal—penetration. Therefore, it is necessary to hide service pages (e.g., phpinfo.php, temp.php, test.php.) and service information displayed in error messages.
45. Turn off unnecessary services. Block unused ports, configure a firewall, and/or Web Application Firewall (WAF).
46. Restrict access to the administrator panel from the internet and public networks.
47. Change your site and server access passwords regularly.
48. Use secure server access methods for file transfer and management (SFTP, SSH, etc.).
49. Configure input filtering in web forms.
50. Back up your site and database (if any) regularly.
51. It is quite common to observe the location of several unrelated web resources on one virtual machine. For example, a website and an old version of the website, or a new test version. The old version is not supported and has old vulnerabilities, the test version is incomplete and also vulnerable, while they are accessible from the internet. Due to the vulnerabilities of these web resources, attackers gain unauthorized access to the main web resource.[26]
52. Configure MS Office security settings,[27] CorelDRAW, Notepad++.
53. Take safety measures for organizing remote work.[28]
54. Foster partnerships between academic institutions, government and international organizations to improve information sharing, establish

[26] CERT-UA, "Рекомендації CERT-UA з безпеки вебресурсів." January 27, 2020, https://cert.gov.ua/recommendation/19.

[27] CERT-UA, ”Рекомендації CERT-UA з налаштувань MS Office", https://cert.gov.ua/files/pdf/Recommendations-MSOffice.pdf

[28] CERT-UA, ”Рекомендації щодо організації віддаленої роботи", April 4, 2021, https://cert.gov.ua/recommendation/11388

best practices, and develop regulatory frameworks. Maintain a balance between cybersecurity and the principles of open science, ensuring the accessibility of research and the protection of sensitive data.

55. Address budget constraints by implementing scalable cyber defense solutions and sharing resources across agencies. Increase the stability of institutions by developing internal expertise and attracting support from the state.
56. For scientific institutions engaged in development in the field of security and defense, use legending and additional security measures.

Bibliography

Center for Strategic and International Studies. "Survey of Chinese Espionage in the United States Since 2000." csis.org, March 2023. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

Cary, Dakota. "Academics, AI, and APTs How Six Advanced Persistent Threat-Connected Chinese Universities Are Advancing AI Research". cset.georgetown.edu, March 2021. https://cset.georgetown.edu/publication/academics-ai-and-apts/.

Gaddis, John L. "Intelligence, Espionage, and Cold War Origins." Diplomatic History 13, no. 2 (1989): 191–212.

"COVID-19 Cyber Threats (Update)". cisa.gov, 13 August 2020. https://www.cisa.gov/sites/default/files/publications/202008131030_COVID-19%20Cyber%20Threats%20Update_TLP_WHITE.pdf.

Bannister, Adam. "Bad Education: Universities Struggle to Defend Against Surging Cyber-Attacks During Coronavirus Pandemic." The Daily Swig | Cybersecurity news and views, February 23, 2021. https://portswigger.net/daily-swig/bad-education-universities-struggle-to-defend-against-surging-cyber-attacks-during-coronavirus-pandemic.

Bowen, Mark. "DDoS Attacks Against Educational Resources Increased by More Than 350%, Says Kaspersky – Intelligent CIO Middle East." *Intelligent CIO*, September 15, 2020. https://www.intelligentcio.com/me/2020/09/15/ddos-attacks-against-educational-resources-increased-by-more-than-350-says-kaspersky/.

"Bad Actors Innovate, Extort and Launch 9.7M DDoS Attacks in 2021 According to the Latest NETSCOUT Threat Intelligence Report." ir.netscout.com, March 22, 2022. https://ir.netscout.com/investors/press-releases/press-release-details/2022/Bad-Actors-Innovate-Extort-and-Launch-9.7M-DDoS-Attacks-in-2021-According-to-the-Latest-NETSCOUT-Threat-Intelligence-Report/default.aspx.

Coker, James. "Top UK Universities Recovering Following Targeted DDoS Attack." Infosecurity Magazine, February 20, 2024. https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/.

"Data Incident." University of Minnesota System. Дата звернення, July 29, 2025. https://system.umn.edu/data-incident.

"IU Reports Records Exposed in Data Breasch Are Public Domain." *Indiana Public Media*. July 13, 2023. https://indianapublicmedia.org/news/indiana-university-suffers-second-data-leak-this-year.php.

"Notice of Data Breach | Communications | University System of Georgia." University System of Georgia, April 14, 2024. https://www.usg.edu/news/release/notice_of_data_breach.

Cluley, Graham. "US College Set to Permanently Close After 157 Years, Following Ransomware Attack." Hot for Security, May 11, 2022. https://www.bitdefender.com/en-us/blog/hotforsecurity/us-college-set-to-permanently-close-after-157-years-following-ransomware-attack.

Zelko, Scott. "A Recap of Recent Cybersecurity Incidents at Universities." Schellman Compliance, November 14, 2023. https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023.

Ibrahim, Fares. "Importance of Cybersecurity in Educational Institutions." July 2024. https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions?channel=doi&amp;linkId=66a0b0fe5919b66c9f683dbe&amp;showFulltext=true.

Oleniak, Liliana. "Russia Strikes Educational Institution With Ballistic Missiles in Poltava: 41 Killed, 180 Wounded." RBC-Ukraine, March 9, 2024. https://newsukraine.rbc.ua/news/russia-strikes-educational-institution-with-1725366089.html.

“A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide.” blog.checkpoint.com, October 18, 2024. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

“CERT-UA Фактор кібербезпеки.” cert.gov.ua, April 1, 2024. https://cert.gov.ua/recommendation/6278274.

“VirusTotal.” VirusTotal. Accessed July 29, 2025. https://www.virustotal.com/gui/home/upload.

“CERT-UA Основні правила кібергігієни.” cert.gov.ua, December 13, 2018. https://cert.gov.ua/recommendation/31.

“CERT-UA Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення.” cert.gov.ua, July 21, 2020. https://cert.gov.ua/recommendation/2502.

“Managing Your Passwords.” NCSC. Дата звернення July 29, 2025. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers.

“Рекомендації державного центру кіберзахисту.” scpc.gov.ua, January 24, 2022. https://scpc.gov.ua/uk/recommendations/129.

CERT-UA. Рекомендації з самостійного пошуку та ліквідації веб-шеллів. https://cert.gov.ua/files/pdf/CUA-14-06R.pdf.

“CERT-UA рекомендації CERT-UA з безпеки вебресурсів.” cert.gov.ua, January 27, 2020. https://cert.gov.ua/recommendation/19.

CERT-UA. Рекомендації CERT-UA з налаштувань MS Office. https://cert.gov.ua/files/pdf/Recommendations-MSOffice.pdf.

CERT-UA. Рекомендації щодо організації віддаленої роботи. April 4, 2021. https://cert.gov.ua/recommendation/11388.

https://doi org/10 59862/k7m2x9q4r8/04

Chapter 4

Research Data during an Armed Conflict: An Overlooked Target?

ALEKSI KAJANDER
NATO Cooperative Cyber Defence Centre of Excellence,
Department of Law, Tallinn University of Technology
ORCID: 0000-0001-7164-2973

Abstract: The protection of digital data remains uncertain under international humanitarian law, with some states recognizing digital data as an object, while others do not. Current international humanitarian law primarily protects visible and tangible civilian objects, whereby digital data is not always recognized as an object and as such is subject to fewer protections than corporeal civilian objects. As a result, important civilian datasets may be at risk during an armed conflict, including research data held by educational institutions such as universities. This paper will examine the existing protections for civilian data under international humanitarian law, in particular under Articles 52, 57, and 58 of Additional Protocol I as well as current state positions on the status of data during armed conflict. Furthermore, this paper will offer practical recommendations to educational institutions on how to protect their research data during an armed conflict under current international humanitarian law.

Keywords: IHL, data, object, cyber warfare, cyber operations, research data, armed conflict

Modern armed conflicts, as demonstrated by the Ukraine war, incorporate a significant cyber component in them.[1] Ever since Stuxnet, it has become clear that cyber operations can deliver the same impact as conventional

[1] Lika Lagvilava, "The 2022–2023 Russia Ukraine War and Cyberspace Threats," *Future Human Image* 19 (2023), 43.

weapons and be considered armed attacks under international law.[2] However, while cyber operations can produce physical damage, often their impact is non-physical, such as the deletion or alteration of data. This creates the potential for a loophole in the protection provided by international humanitarian law (IHL) during an armed conflict, as while (physical) civilian objects are protected from attack, it is not quite clear whether data truly qualifies as an object. Although this may potentially affect many different types of data important for civilians, it is perhaps underappreciated that it can compromise significant scientific research data held at universities. This paper will examine the threat to research data during an armed conflict under IHL, and what measures may be recommended for research institutions to minimize their exposure.

Status of Universities under IHL

Under IHL, it is well established that civilian objects are protected and shall not be made the object of an attack under Article 52 of Additional Protocol I to the Geneva Conventions. Some objects, such as medical facilities are subject to additional protection with specific provisions that ensure that not only is it forbidden to attack them, but that they must be respected at all times and that their operation shall not be interfered with.[3] Similarly, objects essential for the survival of the populace,[4] cultural objects, and places of worship have[5] similar broad protections that go beyond merely not attacking. It may therefore be surprising that universities or other such research or educational institutions do not have a similar special protection.[6] Instead, universities and other places of learning or research are treated the same as any other civilian object.

[2] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 342.

[3] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31, Article 19.

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 54.

[5] Ibid, Article 53.

[6] Gregory Bart, "The Ambiguous Protection of Schools under the Law of War – Time for Parity with Hospitals and Religious Buildings," *Georgetown Journal of International Law* 40, no. 2 (2009), 427.

Initially, especially to a non-IHL lawyer, this may seem like trivial differences. However, with the advent of cyber operations during armed conflict, the lack of special protection has become increasingly significant. With cyber operations, the additional protections provided by broader wording such as "shall respect,"[7] "any acts of hostility,"[8] and "render useless"[9] has increased meaningfully. The prohibition against attacking only extends to civilian "objects," which are defined in the 1987 Commentary to Additional Protocol I as "visible and tangible."[10] While this was fine in 1987, since then, "immaterial" digital data, which one arguably cannot see or touch, has become incredibly important in many civilian contexts. As a result, a view that data is not an object under IHL has become prominent,[11] whereby civilian data could, as a result, be subject to a loophole where, as it is not an object, it could be attacked through cyber means, unlike physical civilian objects. Therefore, the previously mentioned broader protections have arguably increased in value as they are wide enough to encompass essentially any hostile activity aimed at them, and hence they arguably provide more protection against cyber operations.

To convey how controversial the classification of data as an object currently is, the available state positions on the Cooperative Cyber Defence Centre of Excellence's (CCDCOE) CyberLaw Toolkit on cyber and international law provide a demonstration. Ten states have provided[12] a position that includes their view on whether data is an object or not under IHL. Six of these consider data as an object,[13] two consider that more discussions are

[7] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31, Article 19.

[8] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 53.

[9] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 54.

[10] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2008.

[11] Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law," *Journal of Conflict & Security Law* 28, no. 2 (2023), 354.

[12] Cyber Law Toolkit, "Scenario 12: Cyber Operations Against Computer Data," accessed November 9, 2024, https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data.

[13] Austria (2024), Costa Rica (2023), Finland (2020), France (2019), Germany (2021), and Romania (2021) (preliminarily).

required and are thus undecided,[14] and finally, two do not consider data as an object.[15] The views of the two states that do not recognize data as an object are rather similar. In both cases, they do not consider data as an object by itself, although if a cyber operation foreseeably causes injury, death, or damage to (physical) objects, they would consider an "attack" under IHL and as such subject it to the applicable rules on targeting.

This miniature snapshot into state opinion is valuable for research facilities to be aware of, as the deletion of research data is unlikely to foreseeably result in a loss of life, injury, or damage to (physical) objects. As such, they must recognize that in the views of some countries it does not receive the same protection under IHL as physical objects, and therefore, they should not expect the same protection as they might for, for example, their buildings. Consequently, as discussions are still ongoing, it would be valuable for research facilities to make their opinions known and contribute to the discussion on the topic.

Lessons from the Ukraine War

With this in mind, the concern for research data becomes readily evident. Moreover, the ongoing armed conflict in Ukraine has already demonstrated that such cyber operations do in fact occur. The Main Directorate of Intelligence of Ukraine's Ministry of Defence reported that two petabytes (200 million gigabytes) of data were deleted from Russia's Far Eastern Scientific

[14] Federal Department of Foreign Affairs. (2021). Switzerland's position paper on the application of international law in cyberspace. https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf; United Nations General Assembly. (2021). Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136, p. 23.

[15] Roy Schöndorf, "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *US Naval War College International Law Studies*, 97 (2021), 401; Jeppe Kjelgaard and Ulf Melgaard, "Denmark's Position Paper on the Application of International Law in Cyberspace," *Nordic Journal of International Law*, 92(3) (2023), 455.

Research Centre of Space Hydrometeorology.[16] Among its other functions, the research center in question provides and handles satellite data and imagery to the Russian Ministry of Defence as well as other departments of the Russian state.[17] The operation raises an important observation that all research facilities should be aware of, that is to say, can they be construed as being "dual use," which may make them targetable from an IHL perspective?

While "dual use" is not technically a formal category of objects under IHL,[18] the concept is useful when discussing objects that have both a military and a civilian use. The appropriate assessment of an object from an IHL perspective is under Article 52 (2) whereby military objects are those which by their "nature, location, purpose, or use make an effective contribution to military action" and which if neutralized provides a "definite military advantage." As noted by the 1987 Commentary, establishments that produce civilian goods that can be used for the benefit of the army have a "dual function" whereby they may be attacked if the definite military advantage anticipated is proportional to the collateral to civilians. This is particularly relevant for research facilities that are expected to enable the production through research of either military technologies, services, or goods, or similar dual-use products that may benefit the armed forces in the future. In such situations, a research facility can be targetable under IHL regardless of the status of data as an object.

Furthermore, under Article 57 (2) of AP I, belligerents have an obligation to choose means and methods that minimize the expected collateral damage to civilians or objects. Therefore, a cyber operation that wipes the research data that may give rise to a military advantage in the future is immensely justifiable compared to kinetic methods, and as such, during an armed conflict might arguably be said to be the preferable means of dealing with such research facilities. For it is difficult to foresee a loss of civilian life when research data is deleted, and no physical damage is produced. As such, it could be argued

[16] Main Directorate of Intelligence (Ukraine), "Знищили ворожу 'планєту' – деталі кібератаки проти центру космічної гідрометеорології рф," January 24, 2024, https://gur.gov.ua/content/znyshchyly-vorozhu-planietu-detali-kiberataky-proty-tsentru-kosmichnoi-hidrometeorolohii-rf.html.

[17] Ibid.

[18] Oona Hathaway, Azmat Khan and Mara Revkin, "The Dangerous Rise of Dual Use Objects in War," *Duke Law School Public Law & Legal Theory Series*, no. 2024–56 (2024), 17.

that the belligerents should if, possible, prefer cyber means in such situations due to Article 52 (2) of AP I over conventional kinetic alternatives to preserve civilian life. Therefore, the cyber threat to research facilities during an armed conflict is significant.

Recommendations for Research Facilities

An often-overlooked aspect of IHL is the obligation for both parties to take precautions against the effects of attacks, as codified under Article 58 of AP I. The passive precautions noted in Article 58 are intended to provide an additional layer of protection to civilians by pre-emptively placing away from harm's way during military operations. In particular, sub-paragraph (b) which requires parties to the "maximum extent feasible" "avoid locating military objectives within or near densely populated areas," should be considered by research facilities. If a research facility is dedicated to such lines of research that can be assessed to give a definite military advantage to the armed forces, they should, where possible, be located away from other parts of such centers that are purely civilian in function and purpose. As per the commentary of 1987,[19] it is clear that this applies to the physical buildings that constitute the potential military object.

However, in the modern context, it would be advisable to extend the interpretation of this obligation not only to the physical building, but also its digital infrastructure. For, if either military or dual-use type research data is located, processed, and stored separately from non-military research data, this in effect translates 58 (b) to the modern environment. This separation would serve as a passive protective measure against a cyber operation targeting research data during an armed conflict. For, if the adversary would conduct a cyber operation intended to alter or wipe data, it would be limited to the separate network or storage that houses the dual-use or military data. Thus, the civilian research should be left unharmed, at least with an adversary who respects the principle of distinction under Article 48 of AP I.

Moreover, even if the data would not be recognized as an object, as it wo-

[19] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2251.

uld take extra effort that must purposefully be targeted towards the civilian data, this would likely violate the "constant care" obligation a belligerent has under Article 57 (1). Under Article 57(1) a belligerent must, in their "military operations," take "constant care to spare the civilian population, civilians, and civilian objects." The word "military operations" is notable as it is broader than the protection against "attacks," which again in the modern context is valuable. For cyber operations may not always be attacks, but they are always "military operations" as this term includes, as per the commentary,[20] "other activities whatsoever carried out by the armed forces," which cyber operations will inevitably fall under.

Thus, it is arguably not possible to justify a purposeful effort to harm civilian data on separate infrastructure or network when the military or dual -purpose data is separate and independent of it. By contrast, if they are housed on the same network, infrastructure, or storage, they are immediately at more risk than if they are housed separately. For an adversary could relatively easily justify wiping all the data they encounter in the system of a research facility that is providing a definite military advantage through its data as being proportionate. This would be due entirely to the fact that no civilian lives or damage to civilian (physical) objects would occur. Furthermore, if an adversary does not recognize data as an object, they may similarly argue that it is not protected under IHL and as such its loss is of no consequence.

Therefore, a practical solution for any research facility is to ensure separation, where possible, between data that may legitimately be targetable due to the provision of a military advantage and purely civilian research data. Moreover, this type of arrangement would be consistent with the requirements of Article 58 of AP I, for those countries that recognize data as an object, and analogously, for those that do not. Consequently, if this is considered in the planning and design of the digital infrastructure in advance, it serves a potent passive precaution against the loss of research data during an armed conflict, even if data itself would not be considered an object.

[20] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2191.

Conclusions

Universities and research facilities do not have special protection during an armed conflict, rather they are protected against attacks the same as all other civilian objects. This creates an issue when it comes to research data, as it is still controversial whether data is an object or not, and therefore protected against attacks. As can be seen from state positions, especially when there are no physical consequences from a cyber operation against data, not all states agree that it would amount to an attack. Therefore, as research data has no special protection, unlike for example, medical data, it is vulnerable during an armed conflict as it is not clear if it is a civilian object. Until the status of data as an object under IHL is confirmed, it is recommended that universities protect their research data during wartime by ensuring, as far as possible, that military and dual-use data is stored separately from the rest of their data. Consequently, universities must recognize this risk to their data during peacetime, and make preparations accordingly in their systems, to avoid a rude awakening during an armed conflict.

Policy Recommendations

Research institutions are recommended to take precautions during peacetime to better ensure their data is safe during an armed conflict. Firstly, wherever possible, militarily relevant or dual-use data should, as far as possible, be isolated and stored separately from purely civilian data. This provides additional protection even though digital civilian data is not protected as such, as belligerents have a constant care duty for the civilian population, and as such must not go out of their way to cause harm to civilians. Consequently, a military operation that purposefully extends to civilian data stored separately from the militarily relevant data would likely violate this constant care obligation. Secondly, institutions should consider storing essential data physically on paper, as it is protected under IHL, unlike digital data. Finally, states should raise the issue internationally, such as during the UN's Open Ended Working Group discussions on international law, with an aim to close the loophole by evolving the interpretation of "civilian object" under IHL. Research institutions should ensure their state's decisionmakers are aware of the issue and encourage them to take action on appropriate international fora as well as formulating and expressing their formal state opinion on the interpretation of IHL in a dedicated public document.

Bibliography

Bart, Gregory. "The Ambiguous Protection of Schools under the Law of War – Time for Parity with Hospitals and Religious Buildings." *Georgetown Journal of International Law* 40, no. 2 (2009).

Cyber Law Toolkit. "Scenario 12: Cyber Operations Against Computer Data." https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data.

Federal Department of Foreign Affairs. "Switzerland's position paper on the application of international law in cyberspace." 2021, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

Federal Government of Germany. "On the Application of International Law in Cyberspace." March 2021, Position Paper of Germany.

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31.

International Review of the Red Cross. (1987) Commentary on the Additional Protocol.

Kjelgaard, Jeppe and Ulf Melgaard. "Denmark's Position Paper on the Application of International Law in Cyberspace." *Nordic Journal of International Law* 92, no. 3 (2023), 446-455.

Lagvilava, Lika. "The 2022–2023 Russia Ukraine War and Cyberspace Threats." *Future Human Image* 19 (2023), 43.

Lehto, Marja. "Finland's views on International Law and Cyberspace." *Nordic Journal of International Law* 92, no. 3 (2023), 456–469.

Main Directorate of Intelligence (Ukraine). Знищили ворожу "планєту" – деталі кібератаки проти центру космічної гідрометеорології рф. 24 January 2024, https://gur.gov.ua/content/znyshchyly-vorozhu-planietu-detali-kiberataky-proty-tsentru-kosmichnoi-hidrometeorolohii-rf.html.

Ministry of Foreign Affairs of Costa Rica. "Costa Rica's Position On The Application Of International Law In Cyberspace." 2021, Position Paper of Costa Rica.

Hathaway, Oona, Azmat Khan and Mara Revkin. "The Dangerous Rise of Dual-Use Objects in War." *Duke law School Public Law & Legal Theory Series*, (2024), 2024–56

Pomson, Ori. "'Objects'? The Legal Status of Computer Data under International Humanitarian Law." *Journal of Conflict & Security Law* 28, no. 2 (2023).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Republic of Austria. "Position Paper of the Republic of Austria: Cyber Activities and International Law." April 2024, Position Paper of the Republic of Austria.

Schmitt, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

Schöndorf, Roy. "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *US Naval War College International Law Studies* 97 (2021), 395–406.

United Nations General Assembly. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136 (2021), 17–23 (Brazil), 75–79 (Romania).

PART II.

CYBERSECURITY AND TECHNOLOGICAL SECURITY IN RESEARCH

https://doi org/10 59862/k7m2x9q4r8/05

Chapter 5

A Systemic Approach to Cybersecurity in International Research Projects. The Role of Digital Platforms

SŁAWOMIR WYCIŚLAK
Institute of Economics, Finance and Management
Jagiellonian University, Kraków, Poland
ORCID 0000-0002-8913-1634

Abstract: Digital platforms have become essential to international research projects. This reliance has amplified cybersecurity challenges in academic environments. A systemic approach is needed to balance open scientific practices with security requirements. This article examines cybersecurity in international research collaborations through three key components: input quality and data sources, data processing methods, and research outputs. By analyzing commonly used research platforms, it identifies critical vulnerabilities in current workflows and proposes strategies for building a robust cybersecurity culture in academic settings. These include comprehensive awareness programs, regular training sessions, shared responsibility frameworks, and academic-private sector collaboration. Digital platforms transform the research ecosystem by enhancing scientific productivity. However, they also introduce new cybersecurity challenges requiring careful mitigation. By adopting a balanced approach, the scientific community can harness digital platforms' potential while safeguarding the integrity and security of international research projects.

Keywords: Cybersecurity, international research collaboration, digital platforms, risk management, data security, academic research infrastructure, open science, cybersecurity culture

Introduction

In an era of increasingly interconnected global research, the importance of robust cybersecurity measures cannot be overstated. This article delves into the intricate landscape of cybersecurity challenges faced by international research collaborations, with a particular focus on the pivotal role of digital platforms. We explore a systemic approach to identifying and mitigating risks across the research lifecycle, from data input and processing to output management. The analysis encompasses key elements such as data integrity, access control, and provenance, while also addressing the unique challenges posed by diverse data sources and collaborative environments. Furthermore, we examine strategies for cultivating a strong cybersecurity culture in academic settings and discuss the transformative impact of digital platforms on the research ecosystem. By adopting a holistic perspective, this article aims to equip researchers and institutions with the knowledge and tools necessary to navigate the complex cybersecurity terrain of modern international research projects.

Systemic Approach to Cybersecurity Threats in Research Projects

In the context of international research collaborations (IRC), the management of inputs, processing, and outputs presents unique cybersecurity challenges. This analysis examines these key system elements, focusing on risk identification, mitigation, and control strategies within the IRC framework.

The utilization of diverse data sources as inputs in IRC introduces cybersecurity vulnerabilities. These include maintaining data integrity across multiple sources, implementing effective access control mechanisms for sensitive information, and ensuring clear data provenance for both reproducibility and security audits.[1] To address these challenges, institutions and researchers must implement robust data management practices encompassing rigorous source verification procedures, secure data transfer protocols, comprehensive metadata management systems, and regular data quality assessments.

Risk identification in this context involves recognizing potential threats to data integrity, confidentiality, and availability. These may include unautho-

[1] Joachim B. Ulven and Gaute Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet* 13, no. 39 (2021).

rized access, data corruption during transfer, or inconsistencies in data formatting across sources.[2] The complexity of these cybersecurity challenges necessitates a systemic approach to risk management in IRC projects, considering the interconnected nature of data sources, research methodologies, and collaborative networks.

Mitigation strategies should focus on implementing multi-factor authentication for data access, utilizing encryption for data transfer and storage, and developing standardized data formatting protocols across collaborating institutions.[3] Control measures should include regular security audits, continuous monitoring of data access logs, and the implementation of intrusion detection systems. By adopting a holistic view, researchers can better anticipate and address potential vulnerabilities, thereby enhancing the overall security and reliability of their research endeavors.[4]

The processing phase in international research collaborations involves the manipulation and analysis of input data, where quality assurance mechanisms are crucial to maintaining data integrity. This phase is essential for ensuring the reliability and validity of research outcomes. Quality assurance and quality control are vital for preventing and correcting errors in data collection. Research data integrity is foundational for rigorous and reproducible research, requiring careful planning and management throughout the data lifecycle, including acquisition, analysis, and preservation.[5]

Standardization of methods is crucial to ensure consistent data handling across different collaborators, especially in international projects. Standardization of methods is paramount in ensuring consistent data handling across diverse collaborators, particularly in international projects where variations in protocols could lead to discrepancies. The European Network for Quality

[2] Zihad Hasan Joy et al., "Advanced cybersecurity protocols for securing data management systems in industrial and healthcare environments," *Global Mainstream Journal of Business, Economics, Development & Project Management* 4, no. 3 (2024), 25–38.

[3] Tirumala Rao Vinnakota, "Systemic Assessment of Risks for Projects: A Systems and Cybernetics Approach," *2011 IEEE International Conference on Quality and Reliability*, 2011, 376–80.

[4] Khanyisile Vilakazi and Funmi Adebesin, *A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies EPiC Series in Computing*, 2023; Yesem Kurt Peker, *Raising Cybersecurity Awareness among College Students*, 2016.

[5] Rebecca Kush et al., "Implementing Single Source: The STARBRITE Proof-of-Concept Study," *Journal of the American Medical Informatics Association: JAMIA* 14, no. 5 (2007), 662–73.

Assurance in Higher Education (ENQA) underscores the significance of such standardization in facilitating cross-border cooperation and mobility within the European Higher Education Area.[6] This standardization extends beyond mere data formats to encompass entire workflows and methodologies. Version control is necessary to manage multiple dataset iterations and analysis scripts, which can be complex across institutions and time zones. Computational resource management must balance powerful data processing capabilities with security considerations, particularly in cloud computing environments.

To address these challenges, researchers should implement standardized data processing workflows, use secure version control systems with robust access management, employ encrypted data storage and transmission protocols, and conduct regular security audits of data processing infrastructure.

The outputs of international research projects encompass not only the immediate results but also their broader impacts on the scientific community and society. Assessing the quality of these outputs requires sophisticated measurement tools and frameworks.[7] From a cybersecurity perspective, the management of research outputs presents several challenges:

1. Intellectual property protection: Safeguarding novel findings and innovations, especially in collaborative projects with multiple stakeholders.
2. Embargoes and controlled release: Managing the timing and extent of result dissemination, particularly for sensitive or potentially dual-use research.
3. Long-term data preservation: Ensuring the security and integrity of research outputs over extended periods.

To address these challenges, institutions should consider implementing robust digital rights management systems, developing clear policies for result dissemination and embargo periods, and investing in secure, long-term data archiving solutions.

[6] ENQA, "Quality Assurance and Internationalisation: State of Play and Perspectives for the Future," 2024, the website of European Network for Quality Assurance in Higher Education, May 8, 2024, https://www.enqa.eu/publications/quality-assurance-and-internationalisation-state-of-play-and-perspectives-for-the-future.

[7] Ulven and Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education".

Strategies for cultivating a robust cybersecurity culture in academic settings are crucial for protecting sensitive data, research, and intellectual property in an increasingly digital educational landscape.

One of the most effective strategies is the implementation of comprehensive and ongoing cybersecurity awareness programs. These programs should be tailored to different stakeholder groups within the academic community, including students, faculty, staff, and administrators. Interactive e-learning modules that demonstrate the consequences of careless cyber habits can significantly increase awareness among college students. Such modules should cover topics such as password security, social engineering awareness, and safe browsing practices. Interactive e-learning modules that demonstrate the consequences of careless cyber habits can significantly increase awareness among college users, particularly when addressing fundamental security concepts and social engineering threats.[8]

Regular training sessions and workshops are essential components of a robust cybersecurity culture. These should be designed to keep all members of the academic community updated on the latest cyber threats and defense mechanisms. By conducting these sessions frequently, institutions can ensure that cybersecurity remains a top-of-mind concern for all stakeholders.

Fostering a sense of shared responsibility is crucial in building a strong cybersecurity culture. As emphasized by the Princeton University case study (ISACA, 2020), it's important to bridge the gap between awareness and genuine concern for cybersecurity. This can be achieved by connecting different audience segments with compelling stories and imagery that demonstrate the real-world impact of cyber threats.

Implementing a multi-faceted approach to skill development is also vital. A strategy that combines education, collaboration, research, and awareness to protect critical infrastructure. This holistic approach ensures that all aspects of cybersecurity are addressed within the academic environment. Leveraging diverse training delivery methods can enhance engagement and cater to different learning preferences. Implementing a multi-faceted approach

[8] Jonathan Hobbs, "Cybersecurity Awareness in Higher Education: A Comparative Analysis of Faculty and Staff," *Issues in Information Systems* 24, no. 1 (2023), 159–69.

to skill development is vital. The Cybersecurity Awareness Framework for Academia emphasizes the importance of structured training modules (CATM) integrated into the academic curriculum, ensuring comprehensive coverage of security awareness topics.[9]

Finally, promoting collaboration between academic institutions and the private sector can facilitate knowledge sharing and the adoption of best practices. Such partnerships can provide valuable insights into real-world cybersecurity challenges and solutions, enriching the academic cybersecurity culture.

The Role of Digital Platforms in the Research Ecosystem

Digital platforms have revolutionized the modern research ecosystem by connecting multiple user groups through shared technological infrastructure. These platforms offer features such as modularity and extensibility, allowing for flexible component integration and expansion. Their role extends beyond technical functionalities to encompass economic and social interactions, fundamentally transforming how scientific collaborations are conducted and data is managed.[10] Cloud computing has emerged as critical tools, enhancing the efficiency, security, and transparency of research processes. However, the adoption of these platforms also introduces new cybersecurity challenges that require careful consideration and mitigation strategies.

Figure 1 illustrates the complex web of cybersecurity challenges facing digital platforms in research ecosystems. The mind map effectively visualizes five major interconnected areas of concern: Digital Divide, Regulatory Compliance, Data Breaches, IP Ownership, and Unauthorized Access. Each of these core challenges branches into specific issues that require careful consideration. The Digital Divide node highlights resource inequalities and limited access to tools, while Regulatory Compliance emphasizes jurisdictional conflicts and fragmented policies. Data Breaches point to centralized data risks and sensitive information exposure. IP Ownership addresses credit disputes and blurred attribution, which is particularly relevant in colla-

[9] Mohammed Khader, Marcel Karam, and Hanna Fares, "Cybersecurity Awareness Framework for Academia," *Information* 12, no. 10 (2021).

[10] Mark de Reuver, Carsten Sørensen, and Rahul C. Basole, "The Digital Platform: A Research Agenda," *Journal of Information Technology* 33, no. 2 (2018).

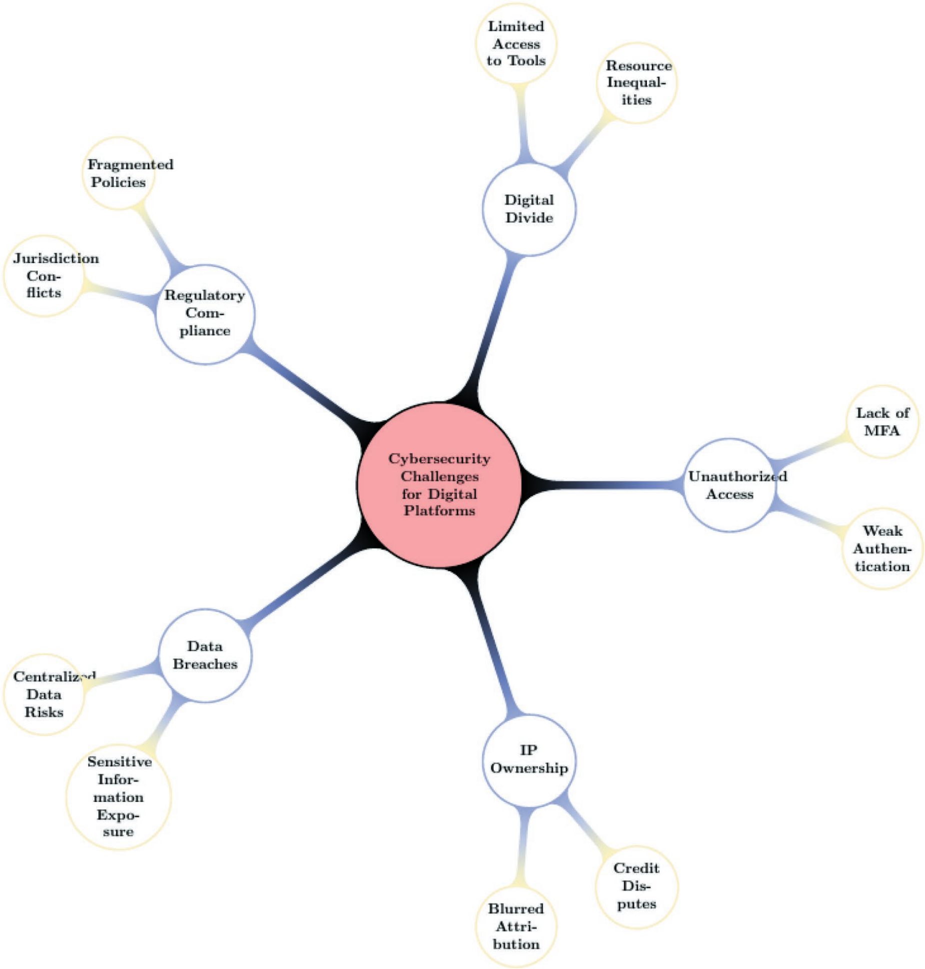

Figure 1. Cybersecurity Challenges in Digital Research Platforms. A Mind Map of Key Vulnerabilities.

borative research environments. The Unauthorized Access branch identifies weak authentication and lack of multi-factor authentication (MFA) as critical vulnerabilities. This visualization complements the discussion of digital platforms in the research ecosystem by mapping out the specific cybersecurity challenges that need to be addressed when implementing and managing digital research platforms.

Digital platforms significantly enhance scientific productivity by streamlining workflows and reducing barriers to collaboration. Cloud-based tools such as Jupyter Notebooks enable researchers to share not only data but entire analytical workflows, promoting reproducibility and accelerating the pace of discovery.[11] This level of transparency and collaboration was previously unattainable in traditional research paradigms. Platforms such as the Open Science Framework (OSF) provide comprehensive infrastructure for managing entire research projects, from preregistration to data archiving. This approach ensures that scientists with diverse specialties can contribute at various stages of the research process, maximizing the utilization of expertise across disciplines.[12]

While digital platforms offer numerous benefits, they also present significant risks that must be addressed. The centralization of research data increases the potential impact of data breaches, potentially exposing sensitive information to unauthorized access.[13] The open nature of many platforms can blur the lines of intellectual property ownership, requiring scientists to navigate complex issues of attribution and credit.[14] Additionally, the digital divide may exacerbate existing inequalities in the scientific community, potentially marginalizing researchers from resource-limited institutions or regions.[15]

A critical yet often overlooked aspect of digital platforms in research ecosystems is the inherent power asymmetry between platform owners and complementors, which introduces additional cybersecurity considerations. Platform owners possess disproportionate control over the technological infrastructure, governance mechanisms, and data access policies, creating a significant power imbalance in the research ecosystem. This asymmetry becomes particularly concerning when platform owners can unilaterally enforce changes in security protocols or access conditions that may impact ongoing research collaborations. The relationship between platform owners and rese-

[11] Thomas Kluyver et al., "Jupyter Notebooks—a Publishing Format for Reproducible Computational Workflows," I*nternational Conference on Electronic Publishing*, 2016.

[12] Erin D. Foster and Ariel Deardorff, "Open Science Framework (OSF)," *Journal of the Medical Library Association* 105, no. 2. (2017), 203–206.

[13] Katherine Akers and Jennifer Doty, "Disciplinary Differences in Faculty Research Data Management Practices and Perspectives," *International Journal of Digital Curation* 8, no. 2. (2013), 5–26.

[14] Thomas Lemieux, "Big Data, Little Data, No Data: Scholarship in the Networked World," *Canadian Journal of Communication* 42, no. 1. (2017).

[15] Louise Bezuidenhout et al., "Beyond the Digital Divide: Towards a Situated Approach to Open Data," *Science and Public Policy* 44, no. 4. (2017), 464–475.

arch complementors is further complicated by the shared objective of providing value to the scientific community while maintaining robust security measures. These power dynamics can affect how security protocols are implemented, potentially creating vulnerabilities if complementors lack sufficient autonomy to implement additional security measures or if platform owners prioritize scalability over security concerns. Understanding and addressing these power asymmetries is crucial for developing comprehensive cybersecurity strategies that protect both platform integrity and research data while ensuring equitable participation in international research collaborations.

To mitigate these risks, the scientific community must adopt a proactive approach. Implementing robust cybersecurity measures, including end-to-end encryption and multi-factor authentication, is crucial for protecting sensitive research data. Clear guidelines for data sharing and intellectual property rights in collaborative digital environments must be developed. Investing in open-source platforms and infrastructure can reduce dependence on commercial entities and promote equitable access. Providing training in digital literacy and data management ensures that all scientists can effectively navigate and utilize digital platforms. Encouraging the development of AI-powered tools can help researchers manage information overload and identify relevant collaborations.

By addressing these challenges, the scientific community can harness the full potential of digital platforms while mitigating associated risks. This balanced approach will ensure that the complementary nature of scientists in digital environments continues to drive innovation and discovery in an increasingly interconnected world. As digital platforms continue to evolve, ongoing research and adaptation of best practices will be essential to maintain the integrity and security of international research projects while maximizing the benefits of these transformative technologies.

Summary

This article explores the critical intersection of cybersecurity, international scientific collaboration, and digital research platforms. It examines the complex interplay between open scientific practices and security requirements

in academic environments, focusing on three key components: input quality and data sources, data processing methods, and the potential impact of research outputs. The study identifies critical vulnerabilities in current research workflows and proposes strategies for cultivating a robust cybersecurity culture in academic settings. These strategies include implementing comprehensive cybersecurity awareness programs, conducting regular training sessions and workshops, fostering a sense of shared responsibility, and promoting collaboration between academic institutions and the private sector. The article also highlights the transformative role of digital platforms in the research ecosystem, emphasizing their ability to enhance scientific productivity while introducing new cybersecurity challenges that require careful consideration and mitigation strategies. By addressing these challenges and adopting a balanced approach, the scientific community can harness the full potential of digital platforms while safeguarding the integrity and security of international research projects in an increasingly interconnected world.

Policy Recommendations

Academic institutions should implement comprehensive cybersecurity awareness programs tailored to different stakeholder groups, including regular training sessions and workshops that address emerging cyber threats. Research institutions must establish clear data governance frameworks that balance open science principles with robust security measures, including standardized protocols for data sharing and access control. Government agencies should develop and enforce consistent cybersecurity standards for international research collaborations while providing adequate funding for security infrastructure and training programs. Digital platform providers must implement enhanced security features, including end-to-end encryption and multi-factor authentication, while ensuring equitable access across the global research community. International cooperation between academic institutions and private sector cybersecurity experts should be promoted to facilitate knowledge sharing and the adoption of best practices.

Bibliography

Akers, Katherine and Jennifer Doty. "Disciplinary Differences in Faculty Research Data Management Practices and Perspectives." *International Journal of Digital Curation* 8, no. 2. (2013): 5–26.

Bezuidenhout, Louise, Sabina Leonelli, Ann Kelly and Brian Rappert. "Beyond the Digital Divide: Towards a Situated Approach to Open Data." *Science and Public Policy* 44, no. 4. (2017): 464–475.

European Network for Quality Assurance in Higher Education. "Quality assurance and internationalisation: state of play and perspectives for the future." ENQA, May 8, 2024. https://www.enqa.eu/publications/quality-assurance-and-internationalisation-state-of-play-and-perspectives-for-the-future (access at 16.07.2025).

Foster, Erin D. and Ariel Deardorff. "Open Science Framework (OSF)." *Journal of the Medical Library Association* 105, no. 2. (2017): 203–206.

Hobbs, Jonathan. "Cybersecurity Awareness in Higher Education: A Comparative Analysis of Faculty and Staff." *Issues in Information Systems* 24, no. 1 (2023): 159–69.

Joy, Zihad Hasan, Siful Islam, Md Atiqur Rahaman and Md Haque. "Advanced cybersecurity protocols for securing data management systems in industrial and healthcare environments." *Global Mainstream Journal of Business, Economics, Development & Project Management* 4, no. 3 (2024): 25–38.

Khader, Mohammed, Marcel Karam and Hanna Fares. "Cybersecurity Awareness Framework for Academia." *Information* 12, no. 10 (2021).

Kluyver, Thomas, Benjamin Ragan-Kelley, Fernando Pérez, Brian E. Granger, Matthias Bussonnier, Jonathan Frederic, Kyle Kelley et al. "Jupyter Notebooks—a Publishing Format for Reproducible Computational Workflows." *International Conference on Electronic Publishing*, 2016.

Kush, Rebecca, Liora Alschuler, Roberto Ruggeri, Sally Cassells, Nitin Gupta, Landen Bain, Karen Claise, Monica Shah and Meredith Nahm. "Implementing Single Source: The STARBRITE Proof-of-Concept Study." J*ournal of the American Medical Informatics Association: JAMIA* 14, no. 5 (2007): 662–73.

Lemieux, Thomas. "Big Data, Little Data, No Data: Scholarship in the Networked World." *Canadian Journal of Communication* 42, no. 1. (2017).

Peker, Yesem Kurt. "Raising Cybersecurity Awareness among College Students." 2016.

Reuver, Mark de, Carsten Sørensen and Rahul C. Basole. "The Digital Platform: A Research Agenda." *Journal of Information Technology* 33, no. 2 (2018).

Ulven, Joachim B. and Gaute Wangen. "A Systematic Review of Cybersecurity Risks in Higher Education." *Future Internet* 13, no. 39 (2021).

Vilakazi, Khanyisile and Funmi Adebesin. *A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies EPiC Series in Computing*, 2023.

Vinnakota, Tirumala Rao. "Systemic Assessment of Risks for Projects: A Systems and Cybernetics Approach." *2011 IEEE International Conference on Quality and Reliability*, 2011, 376–80.

https://doi org/10 59862/k7m2x9q4r8/06

Chapter 6

Cyberthreats to the Science and Research Sector as a Challenge to National Security and Economic Competitiveness[1]

IZABELA ALBRYCHT
AGH University of Krakow

Abstract: This chapter argues that escalating cyber-attacks against universities and research organizations have become a strategic challenge affecting national security and economic competitiveness. It links the sector's growing exposure to the industrialization of cybercrime and intensifying geopolitical techno-rivalry, emphasizing risks of disruption, data theft, and cyberespionage targeting intellectual property and dual-use research. The chapter outlines priority response measures, including EU-level research security initiatives, NIS2-driven compliance, stronger institutional governance, SOC capabilities, supply-chain risk management, and systematic cyber-resilience building within academia.

Keywords: cybersecurity; universities; research security; cyberespionage; intellectual property; hybrid threats; NIS2; cyber-resilience; SOC; supply-chain risk[2]

Introduction

In an era characterized by the widespread digitalization of public institutions and sectors of the economy, including universities and research organizations, the risk of unintentional disruption associated with the operation of a heavily interconnected and networked digital infrastructure is increasing, as is the

[1] Translated with the support of DeepL.com (free version).

[2] The keywords and abstract of this report is based on the text provided by the Author, but was generated by the Editors.

number of intentional malicious cyber-attacks. The latest statistics indicate an alarming surge in cyber-attacks targeting the academic sector. These incidents are becoming increasingly sophisticated, comparable with those targeting other critical infrastructure sectors, such as financial services and healthcare.

The Expanding Scope of Cyberthreats

The latest records indicate that in Q3 of 2024, the number of cyber-attacks worldwide has reached an all-time high, with a 75% increase compared to the same period in 2023.[3] Data from the same report paints an alarming picture: "The Education/Research sector was the most targeted, with an average of 3,828 weekly attacks, followed by the Government/Military and Healthcare sectors, with 2,553 and 2,434 attacks, respectively."[4] These findings are corroborated by the 2024 Data Breach Investigations Report, which highlights that the education sector "was by far the most impacted, accounting for more than 50% of breached organizations."[5] The report analyzed 30,458 real-world security incidents and confirmed a record-high number of 10,626 data breaches, with 1,537 cases of confirmed data disclosure in educational services.[6]

For these reasons, cybersecurity has become a critical challenge for academic institutions, including universities, which are increasingly falling victim to cyber threats. In 2024, institutions such as the University of Cambridge, Università di Siena, Université Paris-Saclay, Reykjavik University, Berliner Hochschule für Technik, University of Winnipeg, Heinrich-Heine-Universität, Universitätsklinikum Brandenburg, Sveriges lantbruksuniversitet, Kansas State University, and South East Technological University Waterford Campus were among many affected by cyber -attacks.[7] The types of cyber-attacks are varying but among the most wi-

[3] Check Point Team, "A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide," Check Point, October 18, 2024, https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

[4] Ibid.

[5] Verizon, "2024 Data Breach Investigations Report," 2024, https://bakotech.pl/upload/fileuploads/files/2024-dbir-data-breach-investigations-report.pdf.

[6] Ibid.

[7] Bert Kondruss, "Cyber attacks on universities," https://konbriefing.com/en-topics/cyber-attacks-universities.html.

despread are ransomware attacks, password compromise, theft of email accounts, and phishing attacks.[8]

The rise in the number and sophistication of cyber-attacks poses significant threats to the confidentiality and integrity of sensitive data, including the financial information of institutions and the personal data of current and future leaders, professionals, and innovators. Not to mention one of the most critical targets: technological breakthroughs made by the academia. Additionally, cyber disruptions create significant operational risks, jeopardizing the daily functions of science and research organizations, which now rely heavily on digital systems, services, platforms, and infrastructure to educate, communicate, and innovate.

Global Factors Driving the Increase in Cyber-Attacks

Over the last few years, cybersecurity risks have intensified due to two main factors: the rise of a globally operating hacking industry and the escalating confrontation between global powers, with geo-tech[9] rivalry between states as a critical element. The hacking industry has become increasingly professional, more innovative, and better organized, adopting a corporate-like structure. It has also begun offering hacking operations and tools in an "as-a-service" model.[10] Cybercriminals are motivated not only by the potential economic benefits of targeting educational institutions but are also used as proxies by their states' authorities. For some governments, cyber-attacks present an opportunity to disrupt critical public services in other countries and a means to extract cutting-edge technologies that enhance economic competitiveness and development, as well as support national security solutions. This explains why the hacking industry has become increasingly engaged in cyberespionage

[8] Anna Maria Trawinska, Alicja Żok and Jakub Jaworski, "Cyberbezpieczeństwo sektora edukacyjnego," *Biuletyn AGH*, December 2023, https://biuletyn.agh.edu.pl/home/biuletyn/wydania/2023/2023_PDF/189_12_2023.pdf.

[9] Izabela Albrycht and Michał Rekowski, *Geopolitics of Emerging and Disruptive Technologies* (The Kosciuszko Institute, 2020).

[10] Tamas Gaidosch, "The Industrialization of Cybercrime," *International Monetary Fund*, June 2018, https://www.imf.org/en/Publications/fandd/issues/2018/06/global-cybercrime-industry-and-financial-sector-gaidosch?utm_source=chatgpt.com.

and even cyberwarfare.[11] Due to described geo-tech and geopolitical reasons, we have been also observing well-organized ecosystems being developed in many countries, including Russia, China, North Korea, and Iran, to support state-sponsored malicious cyber offensive activities of their governments and militaries, which is adding to that threat landscape even more concerning capabilities.[12] Escalating geopolitical confrontation, particularly evident since the Russian aggression against Ukraine in 2014 and 2022, has led to increased risks, with state-originated cyber-attacks being considered a key tool in hybrid warfare. These attacks are used to sow chaos and disrupt the normal functioning of Western countries and their critical entities. In the Council In recommendations on enhancing research security[13] approved in May 2024, European decision-makers and policymakers emphasized that hybrid threats are affecting the research and innovation ecosystem, potentially leading to technology leakage. To address this, they stressed the need for proper and regular assessments, aimed at enhancing situational awareness among policymakers. This effort should be undertaken in collaboration with the Single Intelligence Analysis Capacity, particularly the Hybrid Fusion Cell, while also considering the contributions of the European Centre of Excellence for Countering Hybrid Threats, the European Union Agency for Cybersecurity, and the European Cybercrime Centre established by EUROPOL, especially regarding cybersecurity threats.[14] The same conclusion was formulated by the British government after the review of the national security threats facing higher education perform at the beginning of 2024 and being presented at the security briefing for vice chancellors from twenty-four UK universities organized by the Deputy Prime Minister of the United Kingdom and attended by the Director General of MI5 and Chief Executive of the National Cyber

[11] Tyson Brooks, "The Professionalisation of The Hacker Industry," *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–99.

[12] Piotr Malachiński et al., "The hidden network. How China unites state, corporate, and academic assets for cyber offensive campaigns," *Orange Cyberdefense*, October 22, 2024, https://research.cert.orangecyberdefense.com/hidden-network/report.html.

[13] Council of the European Union, "Council Recommendation on enhancing research security, 2024/0012 (NLE)," *Council of the European Union*, May 14, 2024, https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf.

[14] Ibid.

Security Centre (NCSC).[15] Among the many concerns to be addressed with special measures, the theft of intellectual property from academic research—particularly research with potential dual-use applications through cyber-attacks—was specifically highlighted.[16]

The growing importance of technologies for geopolitical and geoeconomic standing of the countries is making universities particularly vulnerable to diverse hybrid threats that include cyberespionage activities. The growing importance of technology for the geopolitical and geoeconomic standing of nations is making universities particularly vulnerable to diverse hybrid threats, including cyberespionage activities. Attacks on the academic sector, focusing on the theft of intellectual property and industrial espionage, are closely tied to rapid advancements in emerging and disruptive technologies.[17] Technologies such as artificial intelligence (AI), quantum technologies, autonomous systems, biotechnologies, and many others serve as modern drivers of the economy while also having extensive applications in the military realm and defense industry. Innovations in these critical areas often become targets of cyberespionage before they can be patented. The Council of the European Union has warned that "some of the Union's competitors are increasingly advancing their capabilities in this respect or actively pursuing civil-military fusion strategies." This warning particularly relates to the long-term strategy pursued primarily by the People's Republic of China. The threat is even greater from Russia, which, cut off from Western technologies due to sanctions imposed after its full-scale invasion of Ukraine in 2022, is increasingly turning to cyberespionage to bridge its technological gap.[18] Therefo-

[15] UK Government, "Government to launch new consultation to protect UK universities from security threats," *GOV.UK*, April 26, 2024, https://www.gov.uk/government/news/government-to-launch-new-consultation-to-protect-uk-universities-from-security-threats.

[16] Nathan Williams, "Foreign states targeting UK universities, MI5 warns," *BBC News*, April 26, 2024, https://www.bbc.com/news/uk-68902636.

[17] According to NATO definition emerging and disruptive technology areas are artificial intelligence (AI), autonomous systems, quantum technologies, biotechnology and human enhancement technologies, space, hypersonic systems, novel materials and manufacturing, energy and propulsion, next-generation communications networks. See more: https://www.nato.int/cps/en/natohq/topics_184303.htm (access at 16.07.2025).

[18] Alexander Martin, "Fears grow of Russian spies turning to industrial espionage," *The Record*, September 14, 2022, https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage.

re, the need to address "the risk of undesirable transfer of critical knowledge and technology to third countries, which might be used to strengthen these countries' military capabilities and intelligence services, affecting the security of the Union and its Member States," was also highlighted in the Council Recommendation.

An illustrative example of the current importance of technology for Western countries is the development of an innovation ecosystem for emerging and disruptive technologies initiated by NATO in 2019. This effort led, in 2022, to the establishment of the Defence Innovation Accelerator for the North Atlantic (DIANA), a NATO body aimed at fostering and protecting dual-use and deep technologies to support security and defense purposes. DIANA also plays a key role in fueling triple-helix collaboration among academia, government, and industry.[19] The involvement of universities as accelerator sites affiliated with DIANA, including AGH University of Krakow,[20] Imperial College London,[21] Universidad Politécnica de Madrid,[22] Universität der Bundeswehr München,[23] provides yet another compelling argument to ensure they are protected and secure from external threats.

Responding to Cyberthreats

In response to these threats, systemic measures should be introduced based on a strategic approach clearly formulated at the European Union level and subsequently implemented by EU Member States. Universities and research organizations will soon need to comply with the NIS2 Directive.[24] As pre-

[19] *The Defence Innovation Accelerator for the North Atlantic (DIANA)*, https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana.

[20] The Krakow DIANA Accelerator, the Polish site of NATO DIANA was created jointly by the AGH University of Krakow and Krakow Technology Park. See more: https://diana.krakow.pl.

[21] Imperial College London serves as the DIANA Headquarters. See more: https://www.nato.int/cps/en/natohq/news_213288.htm?selectedLocale=en.

[22] Universidad Politécnica de Madrid is the Spanish site of NATO DIANA. See more: https://www.diana.nato.int/resources/site1/general/diana-affiliated-network-accelerator-sites.pdf.

[23] Universität der Bundeswehr München is the German site of NATO DIANA. See more: ibid.

[24] "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," *Official Journal of the European Union EUR-LEX*, no. 333 (2022): 80–152.

viously mentioned, the Council of the European Union is fully aware of the various threats targeting the research sector, including cybersecurity threats. Therefore, we can expect increased emphasis to be placed on addressing these challenges. The Council Recommendation on enhancing research security also called for strengthening "the evidence base for research security policymaking, through analysis of the threat landscape, including from a cybersecurity perspective."[25] It also suggests regular interactions and collaboration aimed at facilitating "information exchange between research-performing organisations and research-funding organisations on the one hand, and intelligence agencies on the other hand, for example through classified and non-classified briefings or dedicated liaison officers."[26] The document recognizes the threat as critical and emphasizes the need to develop or reinforce "cross-sectoral cooperation within government, notably bringing together policymakers responsible for higher education, research and innovation, trade, foreign affairs, intelligence, and security."[27] Additionally, it proposes practical solutions for targeted institutions to build resilience in the sector, including "regular resilience testing and incident simulations, investment in dedicated in-house research security expertise and skills, assigning research security responsibility at the appropriate organisational levels, and fostering cyber hygiene and a culture in which openness and security are balanced."[28]

Universities should, where possible, allocate a budget to strengthen cybersecurity and build cyber-resilience. Cyber-resilience[29] is an increasingly important aspect of organizational resilience and can be achieved through measures that have been recommended for many years by cybersecurity experts and institutions. These include regular updates of software and systems, strong passwords and multi-factor authentication, regular data backups,

[25] Council of the European Union, "Council Recommendation on enhancing research security".

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] "Cyber-resilience should be understood as a capability that a given enterprise possesses to manage a cyberattack and its effects in a way which retains the operational capacity". See more: Izabela Albrycht, "Cyber-resilience," *A Country's Systemic Resilience in the Digital Era*, ed. Izabela Albrycht, The Kosciuszko Institute, 2022, https://cybersecforum.eu/2022/09/21/new-report-a-countrys-systemic-resilience-in-the-digital-era/ (access at 16.07.2025).

and educating employees to recognize phishing attempts and other cyber and ICT threats. Given the rise in the sophistication and frequency of cyberthreats, advanced threat detection and response systems, along with organizational changes, should be introduced. This includes establishing specialized units in universities to protect scientific and research infrastructure, such as laboratories, supercomputers, data centers, servers, and the data processed across numerous IT systems. Rectors should designate one of their deputies, such as a vice-rector, or appoint dedicated representatives responsible for these processes, granting them broad authority to oversee the cybersecurity system.[30]

There is also a need to update relevant policies and procedures and establish new responsibilities among key decision-makers. As universities continue their digital transformation, they must develop robust cybersecurity policies and procedures, ensure these remain relevant to evolving threats, as well as conduct regular audits and risk assessments targeting the entire supply chain.31 Additionally, universities should perform cybersecurity exercises and implement regular training programs for scientists, researchers, staff, and students.

Many entities in the scientific and research sector are already taking steps to build so-called security operations centers (SOCs). For example, the Security Operation Center in Central Europe Region (SOCCER) consortium, which includes universities from five EU countries in the Central and Eastern Europe (CEE) region—Poland, Czechia, Slovakia, Estonia, and Lithuania—was established to support the development and advancement of SOCs within universities and Research and Technology Organizations (RTOs) in the region. The consortium has been awarded a grant from the Digital Europe Programme.[32]

[30] Dariusz Szostek, "Cyfrowa perspektywa przed uczelniami i instytutami," *Forum Akademickie*, July 3, 2024,
^{h}ttps://forumakademickie.pl/szkoly-wyzsze/cyfrowa-perspektywa-przed-uczelniami-i-instytutami/.

[31] A supply chain is a network of organizations, people, activities, information, and resources that work together to deliver a product or service from the initial stage to the hands of the end consumer or final business recipient. The supply chain includes companies that provide components to key or important entities essential to a given product or service. See more: https://www.biznes.gov.pl/pl/portal/005120#6.

[32] "SOCCER – Cybersecurity for Academic Sector," AGH University of Krakow, accessed July 17, 2025, https://soccer.agh.edu.pl/en/.

Finally, it is essential to increase leadership involvement. University rectors must well recognize that the responsibility for the security and cybersecurity of their institutions ultimately rests on their shoulders. They should take steps to establish an effective management and coordination structure for this critical area of university operations. Cybersecurity considerations should also be a key criterion in the procurement process for ICT and network equipment, as well as in the selection of suppliers and business clients. This issue is underscored by the NIS2 Directive, which emphasizes the risks associated with high-risk vendors and the necessity of conducting third-party cyber risk management. At the same time, they should actively pursue opportunities to secure funding through government and EU programs. A dedicated fund is essential to systematically support the academic sector in developing competencies, resources, and tools to enhance cybersecurity. This could be modeled after existing programs supporting other sectors, such as Poland's "Cybersecure Local Government" (*Cyberbezpieczny Samorząd*) program, which provides targeted assistance to local government units.[33] However, there are many other examples of cybersecurity programs that could be explored and tailored to focus more on the cybersecurity of the Science and Research Sector. These include Programme d'Investissements d'Avenir (France), Plan Cyber (France), Nationale Roadmap Grootschalige Wetenschappelijke Infrastructuur (The Netherlands), and Piano Nazionale di Ripresa e Resilienza (PNRR) (Italy).

Conclusion

The outlook for the near future regarding cybersecurity in Western countries is not optimistic. This includes a significant increase in cyber-attacks targeting the science and research sector, among others. Addressing these challenges requires systemic measures supported by decision-makers and governments and implemented by academic leadership. The situation is further exacerbated by the malicious use of AI, which has already become a tool for cyber-attackers. AI enables them to scale and enhance their operations, such as executing advanced phishing campaigns and creating convincing

[33] "Cyberbezpieczny Samorząd," *Cyfryzacja KPRM*, accessed July 17, 2025, https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-samorzad.

deepfakes.[34] Undoubtedly, the global cybersecurity community is facing many problems and dilemmas, which will require international and intersectoral cooperation to be solved (or at least prepare for and counteract). It is crucial to seek opportunities to highlight the importance of cybersecurity of the research and education institutions to policymakers, decision-makers and other stakeholders. Perhaps the upcoming presidency of Poland in the Council of the EU and its priorities could be the next step towards more secure and resilient universities.

Policy Recommendations

1. Continuation of the direction set up within The Council Recommendation on enhancing research security, particularly through the creation of "cross-sectoral cooperation within government," which should involve policymakers responsible for higher education, research and innovation, trade, foreign affairs, intelligence, and security.
2. Start counter measures in collaboration with NATO and the EU to address universities' vulnerabilities to hybrid threats, including cyberespionage activities. These measures should include risk assessments, incident response protocols, and access to shared resources for threat intelligence.
3. Further support the NATO DIANA network's development by ensuring its security against external threats within accelerators and test centers. Implement safeguards such as advanced threat monitoring systems and secure communication channels.
4. Introduce systemic measures based on a strategic approach clearly formulated at the European Union level, to be implemented by EU Member States. These measures should include proper public budget allocation to strengthen cybersecurity and build cyber-resilience across the sector.

[34] Aleksandr Yampolskiy, "What does 2024 have in store for the world of cybersecurity?," February 15, 2024, https://www.weforum.org/stories/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/. See more: Izabela Albrycht, "Cyberbezpieczeństwo w erze sztucznej inteligencji", in *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*, ed. Wioletta Brzęcka and Robert Siudak, The Kosciuszko Institute, 2022, no. 39, https://ik.org.pl/wp-content/uploads/2023/11/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf.

5. Provide instruments to help the sector comply with the NIS2 Directive, including guidance on risk assessment methodologies, security baselines, and compliance audits tailored to higher education and research institutions.
6. Support capacity building for research security policymaking by enhancing the evidence base through a thorough analysis of the threat landscape, including cybersecurity perspectives. This effort should include:
   - Specialized SOCs for advanced threat detection and response.
   - Cyber threat analysis based on Indicators of Compromise (IOCs).
   - Dedicated units to protect critical infrastructure.
7. Develop a cyber-resilience strategy within the sector's institutions, supported by clear political and administrative commitment from leadership, including vice-rectors or dedicated representatives. This strategy should result in updates to policies and procedures (e.g., procurement processes for ICT and network equipment) and establish new responsibilities among key decision-makers.
8. Promote collaboration with national cybersecurity agencies and relevant bodies to provide additional support for cybersecurity capacity building, particularly for small and medium-sized institutions.
9. Run awareness-building campaigns to promote cyber hygiene and foster a cybersecurity culture within the sector. These campaigns should target all stakeholders, including faculty, staff, and students, and focus on practical measures to prevent and mitigate cyber risks.

Bibliography

AGH University of Krakow. Security Operations Center for Education and Research (SOCeR). https://soccer.agh.edu.pl/en/.

Albrycht, Izabela. “Cyber-resilience.” In *A Country's Systemic Resilience in the Digital Era*, ed. Izabela Albrycht. The Kosciuszko Institute, 2022. https://cybersecforum.eu/2022/09/21/new-report-a-countrys-systemic-resilience-in-the-digital-era/.

Albrycht, Izabela. “Cyberbezpieczeństwo w erze sztucznej inteligencji.” In *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*, editors

W. Brzęcka and R. Siudak. The Kosciuszko Institute, 2022. https://ik.org.pl/wp-content/uploads/2023/11/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf.

Albrycht, Izabela, and Michał Rekowski. *Geopolitics of Emerging and Disruptive Technologies*. The Kosciuszko Institute, 2020.

Biznes.gov.pl. https://www.biznes.gov.pl/pl/portal/005120#6.

Brooks, Tyson. "The Professionalisation of The Hacker Industry." *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–99.

Check Point Research. *A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide*. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

Council of the European Union. *Council Recommendation on Enhancing Research Security*, 2024/0012 (NLE). https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf.

Council of the European Union. *Council Recommendation on Enhancing Research Security*. https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf.

Cyfryzacja KPRM. *Cyberbezpieczny Samorząd.* https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-samorzad.

DIANA Poland. https://diana.krakow.pl.

European Union. *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive). Official Journal of the European Union* L 333 (2022): 80–152.

Gaidosch, Tamas. "The Industrialization of Cybercrime." *International Monetary Fund*, https://www.imf.org/en/Publications/fandd/issues/2018/06/global-cyber-crime-industry-and-financial-sector-gaidosch?utm_source=chatgpt.com.

Kondruss, Bert. "Cyber Attacks on Universities." *KonBriefing Research*, https://konbriefing.com/en-topics/cyber-attacks-universities.html.

Malachiński, Piotr et al. "The Hidden Network. How China Unites State, Corporate, and Academic Assets for Cyber Offensive Campaigns." *Orange Cyberdefense*, https://research.cert.orangecyberdefense.com/hidden-network/report.html.

Martin, Alexander. "Fears Grow of Russian Spies Turning to Industrial Espionage."

The Record, September 14, 2022, https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage.

NATO. *Imperial College London Serves as the DIANA Headquarters*. https://www.nato.int/cps/en/natohq/news_213288.htm?selectedLocale=en.

NATO. *NATO Topics: Defence Innovation Accelerator for the North Atlantic (DIANA)*. https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO. *Universidad Politécnica de Madrid is the Spanish Site of NATO DIANA*. https://www.diana.nato.int/resources/site1/general/diana-affiliated-network-accelerator-sites.pdf.

NATO. *Universität der Bundeswehr München is the German Site of NATO DIANA*. Ibid.

Szostek, Dariusz. "Cyfrowa perspektywa przed uczelniami i instytutami." *Forum Akademickie*, July 3, 2024, https://forumakademickie.pl/szkoly-wyzsze/cyfrowa-perspektywa-przed-uczelniami-i-instytutami/.

Trawińska, Anna Maria, Alicja Żok and Jakub Jaworsk. "Cyberbezpieczeństwo sektora edukacyjnego." *Biuletyn AGH*, December 2023, https://biuletyn.agh.edu.pl/home/biuletyn/wydania/2023/2023_PDF/189_12_2023.pdf.

UK Government. *Government to Launch New Consultation to Protect UK Universities from Security Threats*. https://www.gov.uk/government/news/government-to-launch-new-consultation-to-protect-uk-universities-from-security-threats.

Verizon. 2024 *Data Breach Investigations Report*. https://bakotech.pl/upload/fileuploads/files/2024-dbir-data-breach-investigations-report.pdf.

Williams, Nathan. "Foreign States Targeting UK Universities, MI5 Warns." *BBC News*, April 26, 2024, https://www.bbc.com/news/uk-68902636.

Yampolskiy, Aleksandr. "What Does 2024 Have in Store for the World of Cybersecurity?" *World Economic Forum*, February 15, 2024, https://www.weforum.org/stories/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/.

https://doi org/10 59862/k7m2x9q4r8/07

Chapter 7

Safety and Security of Space-Enabled Education/Learning and Research

MAREK CZAJKOWSKI
Jagiellonian University
ORCID 0000-0003-4276-4984

Abstract: Educational/learning and research satellites can be put in danger in various ways, by various methods, and with varying effects. (1) The process of wearing out or unintentional damage/destruction of satellites concerns individual craft and happens occasionally. (2) Intentional attacks may have a limited and temporary impact on a satellite's operation or may cause serious structural damage resulting in malfunctioning of the satellite or even its fragmentation. (3) An increasing amount of debris in space is resulting in a growing number of collisions which further pollute orbits. This may lead to the so-called Kessler syndrome, a hypothetical situation in which the growing number of collisions in orbit would eventually lead to the cascade effect, rendering whole regions of near-Earth space contaminated to an extent that would make them unusable.

Keywords: International security, space security, space safety, counterspace measures, ASAT weapons, space debris, Kessler syndrome

Executive Summary

Satellites are frequently used for research and education/learning activities, either as carriers of scientific instruments or for supportive purposes (communication, positioning, timing, etc.). Therefore, the safety and security of the operation of these systems directly and indirectly impact the security of research and education/learning activities. Space systems operations may be jeopardized in many ways due to man-made or natural causes, and the severity of related dangers increases in time. This refers particularly to the growing threat of contamination of the space environment caused by remnants of defunct satellites and their parts, launch vehicles, and other items left in space. In most cases, this space debris remains in orbit for a very long time, which means the danger of collisions producing more junk increases and will continue growing at a pace relative to the increase in the number of objects launched into space. It is even possible that a massive cascade effect (i.e., Kessler syndrome) will occur in the near future, resulting in the rapid destruction of a large number of satellites and rendering some orbits unusable. To date, efforts intended to mitigate the degradation of the space environment have not had a significant mitigating effect.

Introduction

Since the beginning of the Space Age, particularly within the last decade or two, numerous important education/learning aids and scientific instruments have been placed in outer space. Furthermore, education facilities such as universities and research centers increasingly rely on communication and positioning, navigation, and timing (PNT) services provided by various satellite constellations. This way, satellite-derived services have become important, in some areas even critically important, for numerous efforts undertaken by educators, students, and scientific teams worldwide. Consequently, the safe operation of space systems has been increasingly vital to the overall security of these activities. However, the safety and security of space infrastructure cannot be taken for granted; on the contrary, it may be jeopardized in many ways. This part of the report will depict existing and prospective threats to space education/learning and research space systems. It will focus on providing a comprehensive list and describing such threats with an accompanying assessment of the likeliness of their occurrence. The follow-on article will also present a broader political and technical context referring to threats to space architecture along with instances of their manifestations.

Safety and Security of Space Systems

By definition, a space system is a set of functionally connected elements designed to provide service or services due to the utilization of a device permanently located in outer space;[1] it is also often referred to as a satellite system. It essentially consists of three segments: (1) a satellite (orbiter) in orbit around the Earth or another celestial body, (2) a ground station used for controlling an orbital craft and receiving/exchanging data from it, and (3) a communication link between these two. This definition applies to all satellite systems, including education/learning and research ones. Usually, multiple satellites are connected with one or more ground stations via radio or laser communication devices, forming a complex structure labelled a constellation. Some space systems provide their services directly to end users on the ground, and user segment such as GPS receivers or satellite phones are also present in these cases.

Almost all objects sent to space circle celestial bodies along trajectories called orbits, which are closed paths of circular or elliptical shape. The vast majority of spacecraft belonging to space systems operate in the Earth's orbits; only a small number of scientific instruments are located around other celestial bodies, including the Sun. Just a few space vessels follow open trajectories that will eventually lead them out of the Solar System. The following argument will refer to space systems in the Earth's orbits where most educational/learning and research activities are being performed.

Satellite systems provide their services in a very complex and hostile outer space environment, which impacts the safety of their operations in many ways. Furthermore, there are various actual and potential situations in which individual segments of space systems may become a target of malicious activity by state or non-state actors. Thus, we refer to the safety of space systems as far as unintentional threats to their operations are concerned and to security with regard to intentional ones. Note that the distinction between "safety" and "security" works well in English, but other languages such as German, French, and Russian do not fully reflect this distinction.

Threats to Education/Learning and Research Space Systems

Due to the characteristics of outer space and human activities there, most of the threats in space can impact educational/learning and research systems

[1] Marek Czajkowski, "Space-Based Systems and Counterspace Warfare," in *Routledge Handbook of the Future Warfare*, eds. Artur Gruszczak and Sebastian Kaempf (Routledge, 2024).

the same way as every other satellite system. There are no specific dangers that might refer only to the part of overall space architecture that is the main subject of this argument; however, some may concern it to a lesser extent. Thus, the list of threats to space systems presented below is not subject-specific; nevertheless, it entails not only a general description of various dangers that may hamper space systems operations but also some considerations referring specifically to educational/learning and research systems. The argument below is, to a great extent, based on the following publications: Global Counterspace Capabilities 2024,[2] Space Threat Assessment 2024,[3] and The Physics of Space Security;[4] other sources will be referred to separately. Threats to space safety and security may be the most generally divided into two already mentioned categories: non-intentional and intentional.

Non-intentional Threats to the Operation of Space Systems

This category of threats entails two subcategories, natural and man-made, and two tiers, primary and secondary.

Primary natural threats stem from the destructive characteristics of the space environment itself. Firstly, every object sent to space is subjected to several types of radiation, which gradually degrade its components, causing damage or even making satellites inoperable and uncontrolled. Occasionally, during so-called solar storms, radiation significantly grows, increasing the possibility of the orbiting craft being damaged. Secondly, low gravity, exposure to vacuum, and solar heat also contribute to the relatively quick degradation of satellite components, which may also cause a loss of control over a craft. Eventually, every satellite ends its operation due to the wearing out of its components caused by the harsh conditions they are subject to in space.

[2] Brian Weeden and Victoria Samson, *Global Counterspace Capabilities* 2024 (Secure World Foundation, 2024). https://www.swfound.org/publications-and-reports/2024-global-counterspace-capabilities-report.

[3] Clayton Swope et al., *Space Threat Assessment* 2024, (Center for Strategic and International Studies, 2024) https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHVGjkxEVeTx3o0.

[4] David Wright, Laura Grego and Lisbeth Gronlund, *The Physics of Space Security* (American Academy of Arts and Sciences, 2005). https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf.

The third primary natural threat to satellite systems stems from the fact that space in the vicinity of the Earth, where most of the human space activity is being conducted, is abundant with micrometeoroids, celestial bodies of a mass less than one gram. Micrometeoroids very frequently impact spacecraft surfaces, contributing to the degradation of the structure of components mentioned above. Additionally, there are less abundant but more dangerous larger bodies called meteoroids, some of which are massive enough to significantly damage or destroy spacecraft on impact. Generally, the smaller the meteoroids are, the more frequently they can be encountered in the Earth's vicinity.

Critically important is that most satellites made inoperable due to natural causes remain in space for a very long time. They slowly change orbit, lose components, and sometimes disintegrate. Consequently, every satellite finally turns into a single piece of space junk or even multiple pieces of debris, which litter the extraterrestrial environment, particularly the most commonly used Low Earth Orbits (LEOs). Consequently, the growing number of uncontrolled satellites and other smaller debris increases the possibility of collisions, which produce even more space junk. Thus, space debris produced due to natural causes form what we can term the secondary threat to space systems, as even the smallest uncontrollably orbiting item, like a tiny splinter of metallic structure, can inflict significant damage on a satellite, particularly on delicate surfaces such as solar panels. Therefore, unintentionally, almost every satellite becomes a threat to others once it goes offline.

The threat of damage or destruction due to collision with space debris applies to every kind of satellite in more or less the same way, relative to the layer of near-Earth space they occupy; the more populated by spacecraft a given layer is, the higher contamination, and consequently, the higher the risk of damage or destruction of orbiting craft (except the lowest usable orbit where atmospheric drag cause deorbiting of debris within weeks or months).

Summarizing to this point, natural conditions in space cause every object permanently stationed in orbit to wear out or be damaged/destroyed due to natural causes in a rather short time. Uncontrolled objects and their fragments, space junk, remain in orbit as a second generation of natural threats:

man-made but created by natural causes. Thus, the risk of damaging and destroying educational/learning and research satellites in the Earth's orbits due to collisions with space junk, particularly in LEO, is not negligible, even if it is not high at the moment. What, however, is particularly important and should be noted at this point in the argument is that the increasing amount of debris, matched with ever-growing space activities, naturally causes a steady increase in the risk of collisions. It may eventually lead to the so-called "Kessler effect," envisioned as early as the late 1970s.[5] This is a hypothetical situation in which the growing number of collisions in orbit would eventually lead to the cascade effect, quickly rendering whole regions of near-Earth space contaminated to an extent that would make them unusable.

Unintentional threats to the operation of space systems may also directly stem from human activities. The first and the most obvious is placing satellites in orbit, as every craft, even before it goes offline, potentially endangers other orbiters. The more of them inhabit a certain orbital plane or certain altitude, the greater the danger of collisions or other interferences. Some orbits are so "crowded" that satellites are frequently forced to alter their flight paths to avoid dangerously close passages with other craft or space debris. Overall, collisions in space are unavoidable, and every one of them further increases the risk of future accidents of that kind. Therefore, the very nature of space, where objects remain for a very long time, even if defunct or torn to pieces, combined with ever-increasing space activities, brings unavoidable threats to all satellites.

Other unintentional threats to satellite systems are technical glitches and human errors, which may result in satellites going offline or even fragmenting before they naturally wear out; nevertheless, they contribute to the expansion of space debris with all the effects described above.

Intentional Threats to the Operation of Space Systems

This section discusses the means used to deprive satellite owners of the benefits stemming from missions space systems perform. In essence, it refers

[5] Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research* Vol. 86, no. A6 (1978): 2637–2646. https://archive.org/details/d14ac03deada9364f8bb1fd236dfdbbacb1d/page/n9/mode/2up.

to situations in which a satellite system is attacked one way or another, leading to interruption or cessation of operation due to temporal or permanent damage or destruction. In general terms, educational/learning and research satellites can be targeted by malicious actors in the same way as other space systems. However, they are less likely to become targets during military operations conducted by nation-states because they are usually much less important from the point of view of strategic concerns. On the other hand, non-state actors may be interested in disrupting educational/learning and research space systems for criminal or commercial reasons. Furthermore, even if not directly targeted, educational/learning and research space systems may suffer the already described secondary effects caused by the increased number of space debris due to combat operations in space. Thus, it is necessary to enumerate all intentional threats to the operation of satellite systems, as all of them may impact the security of space systems either as primary threats or via secondary effects.

Means designed to hamper satellite operations intentionally are usually referred to as "counterspace capabilities"[6] or "counterspace measures" (CSMs).[7] Sometimes, the term "counterspace weapons" is also used to describe all CSMs except cyber intrusion;[8] however, the word "weapon" is reserved for destructive measures in this report. In some classifications, means of providing situational awareness are also included in the list of CSMs.[9]

In the most general terms, counterspace measures may be divided into (1) kinetic weapons designed to damage or destroy satellite system or its parts physically, (2) non-kinetic weapons which may or may not yield physical damage to targeted object, (3) electronic warfare impacting down- or uplink without directly endangering satellite physically, and (4) various means of

[6] Swope et al., *Space Threat Assessment* 2024, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHV-GjkxEVeTx3o0.

[7] Czajkowski, "Space-Based Systems and Counterspace Warfare"

[8] Swope et al., *Space Threat Assessment* 2024, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHV-GjkxEVeTx3o0.

[9] Weeden and Samson, *Global Counterspace Capabilities* 2024, https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.

intrusion through cyberspace. It must also be noted that non-destructive and non-physical measures, which by design are not supposed to bring physical damage or destruction, may ultimately cause such effects due to interference with the satellite's operation.

Various kinetic counterspace measures may affect a space system's ground architecture or its space segment. Ground stations may be attacked by various traditional means of warfare that do not need further description. Space segments may be targeted by what is usually referred to as anti-satellite (ASAT) weapons. They may take the form of ground-based interceptor missiles, called direct-ascent ASAT (DA-ASAT), and space-based, co-orbital (CO-ASAT) systems. They are designed to impact spacecraft directly or with the munition they fire to damage or destroy satellites physically. Attacks of this sort would render a satellite inoperable, turning it into uncontrolled junk, or, highly likely, fragment the targeted craft, contributing to the increased amount of space debris, as described above.

Non-kinetic attacks may involve nuclear explosions, which impact satellites with products such as shockwaves and radiation, or the use of directed energy (DE) devices such as lasers or microwave emitters. If the former is undoubtedly a destructive weapon, the latter need not have to be, which depends on the power of the DE beam. Thus, these weapons may either be destructive, physically impacting satellites in orbit, or they may only render them temporarily inoperative. For example, a laser beam may (1) destroy an observation satellite by an explosion caused by the excessive heat it produces, (2) damage its external structure, rendering it inoperable, (3) permanently blind cameras by destroying their matrices, or (4) only temporarily dazzle the orbiter's optics. So, in the case of DE devices, the distinction between destructive weapons and non-destructive CSMs is somewhat blurred as, in theory, the same systems can be used for both purposes if only their yield can be adjusted. Note that even in the case of a non-destructive attack, a satellite may be rendered uncontrollable, contributing to the contamination of space and increasing the secondary threat the way indicated above.

Electronic warfare impacts the links between space and ground segments of satellite systems. It may be executed in the form of (1) jamming a signal, making the link unusable, or (2) spoofing it, which means that a false signal is being sent to the receiver. In essence, it is a temporary measure as the jamming/spoofing device may be switched on/off, and the process of jamming/spoofing the signal does not affect receivers in any way. However, if the link used to control a satellite is inoperable for a sufficient time due to jamming/spoofing, its systems may malfunction, which could result in turning it into a space junk with all the well-known consequences.

Cyber-attacks may affect satellite systems in many ways. (1) Data exchanged with the ground station with a downlink or uplink may be corrupted, or (2) intercepted for the adversary's benefit, and (3) the orbiter's control software may be penetrated so that the craft is issued false commands, which can ultimately lead to damage or loss of the satellite with all the secondary effects. Cyber intrusions can target satellites in orbit, ground stations, or end users. The effects of cyber interference on space systems may vary from causing satellites to malfunction, denying users access to the system's services, data falsification, and data theft.

As mentioned in the introduction, this report will not provide detailed information on instances of the use of countermeasures. However, it is worth noting that ASAT weapons have not yet been deployed in militarily significant quantities and have never been used except for testing.[10] On the other hand, non-destructive measures are frequently utilized, particularly dazzling, jamming, or spoofing.

Conclusion

Educational/learning and research satellites may be endangered in various ways, by various methods, and with varying effects. Primary threats to space systems, be they intentional or unintentional, do not necessarily have to concern multiple satellites at the same time. The process of wearing out or unintentional damage/destruction of satellites concerns individual craft and happens occasionally. Naturally, the more satellites that orbit the Earth, the more such occasions occur. Intentional attacks causing permanent effects

[10] Weeden and Samson, *Global Counterspace Capabilities* 2024, https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.

may have very limited effects, such as damage to an observation craft's lenses. However, it may also cause serious structural damage, resulting in malfunctioning of the satellite or even its fragmentation. Such destructive attacks may be limited to individual orbiters or may take the form of frequent or even massive warfare in orbit.

As strongly underlined in the argument above, when control over a satellite is lost, whether it has been intentionally destroyed and broken or has just gone defunct out of natural causes, it usually becomes potentially dangerous space junk. The growing probability of collisions with active satellites and space debris is a secondary threat to the safety of space systems. From the point of view of everyday operations and space traffic management, it is the most prominent danger, and it is growing steadily. The more satellites are operating in space now, the more space junk will litter the Earth's orbits in the future. Thus, even without acts of intentional destruction of satellites, the threat to the safe operation of space architecture of every kind is constantly mounting.

It is also worth noting that non-destructive threats are also important from the point of view of the security of education/learning and research process. Every disruption in data flow from or through space architecture or other problems with communication or PNT services might adversely impact the everyday activities of educators and researchers. Additionally, cyber intrusions into space systems may lead to intellectual property theft.

Policy Recommendations

It is imperative for the worldwide scientific community first to understand how threats to space systems impact individual research and education/learning activities, even in fields not related to space science. Secondly, the scientific community must pressure governments to find solutions, seeking alliances with branches of the manufacturing industry and services sectors dependent on satellite systems. Finally, governments and international organizations should prioritize efforts to address the risks associated with increasing contamination of the space environment. International efforts are particularly important, as the danger itself transcends all the earthly boundaries.

Bibliography

Czajkowski, Marek. “Space-Based Systems and Counterspace Warfare.” In *Routledge Handbook of the Future Warfare*, edited by Artur Gruszczak and Sebastian Kaempf Routledge, 2024.

Kessler, Donald J. and Burton G. Cour-Palais. “Collision Frequency of Artificial Satellites: The Creation of a Debris Belt.” *Journal of Geophysical Research* Vol. 86, no. A6 (1978): 2637–2646. https://archive.org/details/d14ac03de-ada9364f8bb1fd236dfdbbacb1d/page/n9/mode/2up.

Swope, Clayton et al. *Space Threat Assessment 2024*. Center for Strategic and International Studies, 2024. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDe-J0EkYnF5W7POfMJHVGjkxEVeTx3o0.

Weeden, Brian and Victoria Samson. *Global Counterspace Capabilities 2024*. Secure World Foundation, 2024. https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf.

Wright, David, Laura Grego and Lisbeth Gronlund. *The Physics of Space Security*. American Academy of Arts and Sciences, 2005. https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf

https://doi org/10 59862/k7m2x9q4r8/08

Chapter 8

Knowledge without Borders: Securing Technology and Data in Global Academic Collaboration

PAWEŁ FRANKOWSKI
ORCID 0000-0003-2143-6279

Abstract: Academic cooperation between third countries and the European Union entails growing risks of unintended knowledge and technology leakage. This paper examines research security challenges arising from fragmented due-diligence practices and increasing internationalization of science. It analyzes institutional constraints, network dynamics, and policy trade-offs, and proposes best practices—including coordinated due diligence and security audits—to safeguard technology transfers while preserving openness and research excellence.

Keywords: Research security, due diligence, technology transfer, academic cooperation, EU research policy, internationalization of science, security audits

The transfer of knowledge and technology from third countries to the European Union within the framework of academic cooperation poses significant risks, such as data and technology leaks, which require proper risk management. The contemporary global exchange of technology necessitates careful preparation of supply chain transfers, encompassing not only logistical aspects but also the secure management of data and technologies. A key element is the implementation of security audits conducted by specialized institutions to identify and mitigate potential threats.

This paper will focus on strategies for minimizing risks by discussing and implementing best practices and procedures for safeguarding technology transfers, with an emphasis on due diligence. Additionally, recommendations will be provided for conducting regular security audits to ensure the integrity of transfers and protect against leaks of strategic technologies. The paper revolves around three general points for discussion on the research security: (1) what is the aim? (2) what are the constraints? (3) if there is a room for spontaneous policy innovations in research security?

Empirical studies show vast evidence for the internationalization of science and therefore the growing risk of unintended errors in research security.[1] Existing international collaboration could be treated as a performance measurement and such factors as the number of third-country scholars or contractors has been quite often treated as a threshold for securing funding. Nevertheless national, and to some extent regional, science structures create powerful obstacles for technology transfer and science transfer, such as national languages, misunderstanding regarding working culture, and particular industrial policies that may treat selected policy areas as priorities for research. These border conditions, which are sometimes not well recognized, constitute both advantages, such as frequent personal contacts or knowledge-sharing in the given networks, and possible problems for research transfer. Without a well-constructed system for research security, a more open regional research community, as advocated by some scholars (Cooke, Gomez Uranga and Etxebarria 1997), is exposed to unintended errors and is perhaps path dependent. Moreover, science networks have, as every network has, all the problems and challenges coming from the uneven distribution of power, ties in the network, and access to resources. Thus, proper network management and analysis of research network capacities is more than relevant to providing research security. Although the EU Council states that "Openness, international cooperation, and academic freedom are at the core of world-class research and innovation,"[2] it also acknowledges the risk of the undesirable and somehow unintended transfer of critical knowledge and technology to countries where fundamental

[1] Stefan Hennemann and Ingo Liefner, "Global Science Collaboration," in *The Handbook of Global Science, Technology, and Innovation*, eds. Daniele Archibugi and Andrea Filippetti (John Wiley & Sons, 2015), 343–363.

[2] Council of the European Union, *Council Recommendation on Enhancing Research Security*, 9097/1/24 REV 1 (Brussels: Council of the EU, May 14, 2024).

European values as well as international obligations can not only be challenged but may be used to strengthen their military capabilities. However, when a general assessment of the problems that may result from fragmented and patchworked national policies is correct, it raises delusive standards for risk assessment and the procedures for due diligence for cooperating institutions and partners. Thus, having a trans-European due diligence agency or portal is more than needed, although the criteria for due diligence are nonexistent. An analysis of the proposal says little about the true importance of such practices and opens a path for rent-seeking when real due diligence will not be performed. When such procedures have been adopted in several British universities, and for example, the University of Reading cannot support any project with third parties from North Korea, Iran, Sudan, South Sudan, Syria, and Crimea, such partners hardly cooperate with European partners. Widening due diligence on other countries' research institutions will be time-consuming and may have a profound impact on productivity and the quality of research. Without clear-cut criteria and the necessary information, EU research institutions risk being trapped in an endless loop. A decision-maker with the authority to grant final approval or veto the decision for moving the project forward will avoid taking any decision (they will "take a position") that would hinder the process of generating any promising research. More information does not necessarily result in better decision-making—also in research security—and therefore, any fundamental trade-offs for research security in the European research area would not happen. Any kind of structured political incentives in order to support or stimulate policymakers in their pursuit of improving policy outcomes are in fact irrelevant without thorough analysis of relevance and the importance of well-crafted structures for due diligence.[3] To gauge the overall magnitude of due diligence for research security and guide further steps, there is an urgent need to establish the role of due diligence actors, and the way they participate in the European science area, either as delegated stakeholders or entrepreneurs. If they have to make rules on behalf of the EU—since a patchworked system of national policies, and perhaps institutions, have

[3] European Commission, *Proposal for a Council Recommendation on Enhancing Research Security*, COM (2024) 26 final (Brussels: European Commission, January 24, 2024).

been considered ineffective—it will lead to a classical transfer of competences at the EU level. Such a classical principal-agent problem raises the question of the selection of agents and their previous performance. In general agents are selected for their ability to reduce transaction costs,[4] while the critical initial condition in research security should be their expertise. In that case, without having experienced agents and a hammered-out procedure, it may be difficult to evaluate the extent to which private agents are autonomous. In consequence, endogenous factors (i.e., lack of clear-cut criteria) may hinder any successful policy of establishing research security. Given that research security does not function as a standalone policy, research institutions cooperate with the business community on knowledge transfer, best practices in data protection, and due diligence instruments. This, in turn, moves us away from a biased policy learning problem, since the business community, which has some level of risk embedded in the business, largely avoids costly experiments or at least learns from their competitors' business choices. Having a good number of cases, when proper due diligence procedures are strongly associated with overall economic performance, we can assume that the entrepreneurial perspective on proper security due diligence would be a promising path for policymaking, with two important comments. First, any kind of policy experiment that gives private authorities full authority in the field of research security, when most due diligence actors have a limited knowledge in the field, may result in a rolling uncertainty on the results. When research institutions and due diligence actors do not agree on the aim and scope of due diligence, any kind of research policy will be put on trial. With learning by doing, which is necessary with such an uncharted area of security policy, the specific objectives (i.e., research security) would not be reached. Second, the degree of complexity, measured by the number of actors involved in the due diligence, could be high, and due diligence actors will tend to lower the number of trials, checks, and question to avoid excessive costs. However, it seems to be necessary to find out a proper ratio between the time and cost of due diligence. If research institutions are involved in the continuous adaptation and tailoring of policies for research

[4] European Commission, *Proposal for a Council Recommendation on Enhancing Research Security*, COM (2024) 26 final (Brussels: European Commission, January 24, 2024).

security, eventually good practices will be established (with a strong emphasis on the complexity of the problem).

The problem of the cost of research security is strictly combined with experience in the field of research security and the lack of effective control of all the inputs. When the quality of research, or institution research capabilities, are controlled (or driven) by the fiat or disciplinary action,[5] any input on research security is controlled by other market actors. The research institution, as a consumer of information, may try avoiding such problem by setting its own research security stewards or separate units in the structure of the institution. However, "reliable information about expected performance is both a costly and a valuable good."[6] What if the cost of gathering further information surpasses both the expected profits from the research outcomes or cumulate the cost of waiting for the final decision? That, again, turns our attention toward the structural problem—perhaps it would more effective if research institutions shared the information on due diligence among partners from the area of research. Gathering information and relevant expertise on security threats through due diligence can be time-consuming and resource intensive. Repeatedly carrying out such due-diligence tasks would place a significant strain on institutional resources. Resource pooling can be an effective instrument for mitigating cost, but effective competition in the research area may lead to competition over relevant information on security. If research actors are tasked with solving coordination problems over defining due diligence, adjusting their behavior, and promoting a certain set of rules for due diligence, this would obviate the need for EU regulations. However, constant emphasis on performance, competitiveness, and building comparative advantage in science opens the way for unnecessary activity.

Policy Recommendations

1. **Establish a Centralized EU Due Diligence Agency:** Create an EU-wide body dedicated to managing and standardizing due diligence practices

[5] Armen A. Alchian and Harold Demsetz, "Production, Information Costs, and Economic Organization," *The American Economic Review* 62, no. 5 (1972), 777.

[6] Ibid., 778.

for technology and data transfers in academic collaborations, ensuring consistent and rigorous security measures across member states.

2. **Implement Comprehensive Security Audits:** Mandate regular, independent security audits for all academic collaborations involving technology transfer to identify vulnerabilities and ensure the integrity of research and data management processes.
3. **Harmonize National Policies:** Address the fragmentation of national policies by developing EU-wide guidelines for research security, balancing the need for openness in academic collaboration with the protection of sensitive technologies and intellectual property.

Bibliography

Council of European Union, *Council Recommendation on Enhancing Research Security*, 9097/1/24 REV 1, 14.05.2024.

European Commission, *Proposal for a Council Recommendation on Enhancing Research Security*, COM (2024) 26 final, 24.01.2024.

Alchian, Armen A. and Harold Demsetz. "Production, Information Costs, and Economic Organization." *The American Economic Review* 62, no 5, (1972): 777–795.

Green Jessica F. *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton University Press, 2014.

Hennemann, Stefan and Ingo Liefner, "Global Science Collaboration." In *The Handbook of Global Science, Technology, and Innovation*, John Wiley & Sons, 2015. 343–363.

PART III.

CASE STUDIES: CHINESE AND RUSSIAN INFLUENCE

https://doi org/10 59862/k7m2x9q4r8/09

Chapter 9

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

MARCIN PRZYCHODNIAK
The Polish Institute of International Affairs
ORCID: 0000-0002-9685-219X

Abstract: The article describes and analyses the “China Initiative” program by the US Department of Justice applied between 2018 and 2022 as an instrument to counter threats in academic cooperation with China. Introduced by the Trump administration and strongly politically motivated, it had, however, a limited impact on raising the security level of scientific research and the research community in the United States against threats originating from China. The article also focuses on an analysis of further policy in this area by the Biden administration, as well as possible plans after inauguration of Donald Trump’s second term. The subjects of the analysis are both “soft” threats (talent acquisition, influence on debate, promotion of political narratives) as well as “hard” threats (scientific espionage, intellectual property theft). The final part of the article is devoted to referring to similar challenges faced by actors in the European Union, with the inclusion of relevant recommendations for the EU and member states arising from the experience of the “China Initiative.”

Keywords: Trump, education, security, research, China, espionage, technology, soft power

The "China Initiative" was a US Department of Justice (DOJ) program launched by the Trump administration in 2018. It was intended to be an effective tool of the DOJ in the fight against Chinese activities in the illegal acquisition of trade secrets, research results—in general: the unfavorable influence of China from the point of view of US interests on scientific and research cooperation between the US and China. Underlying the establishment of the initiative were the findings of reports by the *US Trade Representative* published after investigations into Chinese trade practices under Section 301 of the Trade Act of 1974.[1] They found Chinese practices to be unjustifiable and concluded that a stronger US response was needed.[2]

The "China Initiative" was to focus on identifying and prosecuting those involved in the theft of trade secrets, hacking (obtaining illegal information from computer networks) and economic espionage, but also protecting critical infrastructure against threats from Chinese investment involvement. A separate thread was the compromises made by US-based companies in their supply chains, to the benefit of Chinese entities and China's state interests, and inconsistent with US interests. Key from the DOJ's perspective, however, was activity involving the scientific and academic community. Taking a leading role in implementing the initiative was the National Security Division, a body specially created within the DOJ after the September 11, 2001, terrorist attack,[3] with the participation of a special prosecutor and the FBI.

The priorities of the "China Initiative" were as follows:

1. Identifying trade secret theft cases and supervision of their handling.
2. Developing a strategy that strengthens the protection of "non-traditional actors" (scientists in laboratories, universities, and industrial

[1] This gives the US Trade Representative the authority to conduct investigations and resulting decisions when partners violate existing trade agreements with the US "Section 301 of the Trade Act of 1974," *Congressional Research Service*, May 13, 2024, https://www.congress.gov/crs-product/IF11346.

[2] "Information about the Department's Justice China Initiative and a compilation of China-Related prosecutions since 2018," February 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (access at "Information about the Department's Justice China Initiative and a compilation of China-Related prosecutions since 2018," February 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

[3] Ibid.

security) from being co-opted by the Chinese in technology transfers inconsistent with US interests.

3. Educating university and college employees about threats to academic freedom and freedom of debate posed by Chinese influence, presence, and funding by PRC entities on campus.
4. Foreign Agent Registration Act reference[4] to unregistered entities trying to promote China's political agenda.
5. Equipping justice agencies with new tools and information to strengthen awareness of threats.
6. Implementing the Foreign Investment Risk Review Modernization Act[5] in Justice Department activities.
7. Identifying risks to supply chains, particularly from the telecommunications sector's perspective, ahead of the period of change associated with the implementation of the 5G standard.
8. Identifying Foreign Corrupt Practices Act[6] (FCPA) cases involving Chinese companies' competition with American companies.
9. Strengthening pressure on China to improve the quality of Chinese responses to US inquiries Mutual Legal Assistance Agreement[7] or legal assistance.
10. Assessing the obligations of administrative and legislative bodies in the US to protect national resources from external economic aggression.[8]

Between the 2018 and 2021 the Department of Justice launched more than fifty investigations under the initiative. They covered a broad spectrum of

[4] The Foreign Agent Registration Act is a 1983 law requiring registration in the US of entities whose activities are related to the operation of a foreign country.

[5] The Foreign Investment Risk Review Modernization Act is a 2018 law that strengthens the authority of the Committee on Foreign Investment (led by the Treasury Secretary) to address risks from investments in the United States to US security.

[6] The Foreign Corrupt Practices Act is a 1977 law prohibiting US citizens and entities from corrupting foreign politicians and officials.

[7] The 2000 agreement between the US and China on legal cooperation and exchanging information on cases of interest to the legal authorities of both countries and conducted by the judiciary of the other country.

[8] Information about the Departments of Justice China Initiative and a compilation of China-Related prosecutions since 2018.

issues, including the investigation of Huawei's vice president, the prosecution of a former CIA officer accused of spying for China,[9] to engineers allegedly secretly exporting advanced semiconductors to China.[10] Special activities under the initiative (in addition to investigations) were also undertaken by the FBI in an effort to persuade the US academic and scientific communities to cooperate more with justice authorities. One of the tools in this context was to be the Domestic Security Alliance Council, which, based on cooperation between public and private entities, was to improve cooperation between the FBI, the Department of Homeland Security, and academia, among others.

In February 2022, after Joe Biden's inauguration, the new leadership of the National Security Division at DOJ modified the operation of the "China Initiative."[11]" China remained a key target, but investigations were to focus this time not on, as the new director of the division put it, "Chinese people, or people of Chinese descent," but activities conducted by Chinese government, or representatives of the Chinese Communist Party.[12] However, this was mainly a rhetorical change, in response to public criticism of previous DOJ actions. It marked the theoretical end of the "China Initiative," but in fact the new administration did not abandon countering threats from China related to research cooperation, industrial espionage, or the presence of Chinese entities and scientists in US academic centers, as well as US scientists collaborating in China. It upheld as guidance for the scientific community the guidance (US Presidential Memorandum) published at the end of Donald Trump's administration mandating stronger protection of the research and

[9] "Former CIA Officer sentenced to prison for espionage," *Press Release, Department of Justice*, May 17, 2019, https://www.justice.gov/archives/opa/pr/former-cia-officer-sentenced-10-years-prison-conspiracy-commit-espionage.

[10] "Electrical Engineer Convicted of Conspiring to Illegally Export to China Semiconductor Chips with Missile Guidance Applications," *Press Release, Department of Justice*, July 2, 2018, https://www.justice.gov/archives/opa/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips-missile.

[11] "Assistant Attorney General Matthew Olsen Delivers Remarks on Countering Nation-State Threats," *Speech, Department of Justice*, February 23, 2022, https://www.justice.gov/archives/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats.

[12] Mitch Ambrose, "Discarding ‚China Initiative' Label, DOJ Pledges Prosecutorial Restraint on Research Security," AIP, February 25, 2022, https://www.aip.org/fyi/2022/discarding-china-initiative-label-doj-pledges-prosecutorial-restraint-research-security.

development sector from foreign influence.[13] The memorandum had significant implications for the academic community by clarifying for scientific agencies and federal institutions the rules and procedures for reporting on cooperation with Chinese entities in situations of federally funded research. Previously, the DOJ, as part of the "China Initiative," undertook several investigations of scientists who were alleged to have concealed such cooperation, and one investigation even resulted in a conviction.[14] A large number of investigations started previously were also continued at the DOJ during the Biden administration. In this context, while there is continuity between administrations within US institutions, the differences are largely rhetorical. At the same time, the expected[15] radicalization of policy toward China in Donald Trump's second term, the announcements of upcoming appointments to the White House and State Department, as well as recent initiatives by Republicans in Congress signal that a return to earlier ideas, only of a broader nature, is possible from January 2025. This is indicated by the ready-made legislation already passed by Congress, where, also with the participation of Democrats, a majority was found for a bill postulating a return to the "China Initiative," this time under the name "CCP Initiative."[16] According to its provisions, the DOJ and the National Security Division are to no longer only investigate the risks of scientific cooperation with PRC entities, but generally the course and fruits of cooperation with entities affiliated with, or originating from, the activities of Chinese Communist Party.

[13] "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," *White House*, January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[14] "Harvard University Professor Convicted of Making False Statements and Tax Offenses," *Press Release, Department of Justice*, December 21, 2021, https://www.justice.gov/usao-ma/pr/harvard-university-professor-convicted-making-false-statements-and-tax-offenses.

[15] This would be indicated not only by announcements during the election campaign (mainly concerning the need for more decisive action, mainly in the trade sphere), but also by preliminary announcements of future appointments to the positions of Secretary of State or National Security Advisor during Donald Trump's second term in the White House. The transactional nature of the policy, the willingness to make concessions, as well as the presence among the advisors of people who are highly dependent on economic cooperation with the PRC, remain issues.

[16] "H.R. 1398 - Protect America's Innovation and Economic Security from CCP Act of 2024," US Congress, September 16, 2024, https://www.congress.gov/bill/118th-congress/house-bill/1398.

Assessment and Outlook

The "China Initiative" was an example of a political response to a correctly diagnosed problem—China's influence and information extraction in industrial espionage, trade secrets, and scientific research. It not so much concerned trade and the activity of the companies themselves, but an earlier stage, i.e., creation and research carried out within colleges, universities, and the cooperation of scientists. In China, the activity aimed at acquiring this kind of information has been inscribed for years in an organized and structured process managed by the institutions and bodies of the Chinese Communist Party, written into the state's development plans,[17] as one of the elements of supporting the development of the Chinese economy, both in terms of technical solutions, patents, but also building a positive image of cooperation with China.[18] This includes military technologies, by virtue of the extensive cooperation between Chinese civilian universities and the People's Liberation Army (PLA).[19] It is undergoing development, embracing new fields and environments; it is also an important element of China's foreign policy and the PRC's relations with countries of the so-called Global South.[20] From this angle, China is also active in Central European countries using scholarships to build a positive atmosphere of cooperation (e.g., toward the management of universities[21]), convincing cooperation in

[17] Among others, "Made in China 2025."

[18] Details of this cooperation related especially to the activities of the CCP's various organs, as well as a list of Chinese universities permanently cooperating with the PRC armed forces can be found in: William C. Hannas and Didi Kirsten Tatlow (ed.), China's Quest for Foreign Technology, Routledge, 2021.

[19] This cooperation is the subject of the "China Defense Universities Tracker" project conducted by the Australian Strategic Policy Institute think tank. The PLA's procedure of sending (secretly) officers on overseas scholarships is described in the report: Alex Joske, "Picking flowers, making honey," Australian Strategic Policy Institute, October 30, 2018, https://www.aspi.org.au/report/picking-flowers-making-honey/.

[20] During the G20 summit in Brazil, in his speech, President Xi Jinping proposed (emphasizing cooperation with Brazil, South Africa, and the African Union), among other things, the establishment of an initiative for cooperation and open access to knowledge. This follows efforts by the Chinese side at the Forum on China–Africa Cooperation (FOCAC) summit in Beijing this year, among others.

[21] Issues of continued cooperation with PRC entities are now of key importance in the framework of the election of a new chancellor of Oxford University (the current one is stepping down at the end of the current academic year), for which the share of international students (46% of all students overall) is an important component of the annual budget.

AI,[22] pledging to finance certain infrastructure (e.g., buildings), and Chinese language courses. The priority of China’s actions in this context, of course, remains in the highly developed economies—the US, Germany, France, Italy, Japan, etc., although the presence of Chinese entities and the associated risks in those economies have a much longer history. A pillar of China’s “opening up to the world” policy has been precisely the search for and acquisition of talent, technology, and investment (as well as natural resources), as a tool for developing its own potential.

By modifying the operation of the “China Initiative,” the Biden administration sought to neutralize the main allegations of racial profiling and the lack of firm criteria (the general nature of priorities) for selecting the cases its investigations would cover. With its formal nature and the publicity of its actions by parts of the media, the initiative may indeed have resulted in discrimination against innocent scientists or workers of Chinese descent. It was also supposed to be ineffective, which was confirmed by some analyses indicating a small number of successful investigations (about a quarter of all investigations launched). According to the *MIT Technology Review*,[23] the main allegations against it dealt primarily with politics (90% of those investigated were American of Chinese descent), as well as the unspecific nature of the selection of cases.[24] US policy during the Biden administration responded to the same threats, but with slightly different instruments than the ones included in the “China Initiative,” although still, as some of the studies point out, most of the prosecutions cases launched earlier were continued. It also helped to establish some of the formal regulations (still however possibly insufficient) concerning the procedures in the research and science cooperation between the US and China institutions, such as *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy* from 2021.

[22] “Budapest university launching partnership with Chinese university with a focus on AI,” Daily News Hungary, October 25, 2024, https://dailynewshungary.com/budapest-university-partnership-chinese/.

[23] Eileen Guo, Jess Aloe and Karen Hao, “The US crackdown on Chinese economic espionage is a mess. We have the data to show it,” MIT Technology Review, December 2, 2021, https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

[24] Ibid.

Conclusion

The evaluation of the "China Initiative" is not clear-cut. It has certainly reinforced awareness of the dangers of Chinese influence and information-gathering activities in dealing with the US research community. However, the manner in which it was conducted and the strong political focus stemming from both the peculiarities of the Trump administration's actions during its first term and the breadth of issues it addressed worked against it, polarizing the research community and further accentuating the dominant role of the state in this context. The media campaign accompanying the initiative, carried out in the modern political reality of polarization and harsh reactions, repeatedly led to misleading accusations compromising the legitimate intentions of the initiative's authors and implementers—inscribing it in political actions, instead of strengthening the US resistance to Chinese initiatives. The timeliness of similar initiatives (regardless of the name, calculated to counter PRC threats) will be a constant, linked to China's activity in its rivalry with the US, and regardless of the declining number of Chinese students in the US, or the steady process of reducing development cooperation between US and Chinese big tech companies or other scientific entities.

From the point of view of the EU and member states, which are equally subject to the actions of Chinese institutions and attempts to illegally obtain information, the "China Initiative" experience argues for the need to accelerate the processes of implementing appropriate safeguards. Such has already become part of the derisking process with European Commission underlying the necessity of securing European research and development. There also are some regulations on threats and security of research (the "EU's Global Approach to Research and Innovation" from 2021), although there is just one working-level oriented directly at China—"Tackling R&I foreign interference" (staff working document in the European Commission). Also convincing are the already known examples of ambiguous involvement of Chinese scientists in information gathering, or the participation of Chinese projects in research and cooperation relevant to, for example, EU security. Some of the risks have a somewhat different face from the realities of the US education system (where the bulk of the most important and prestigious universities—from the point of view of Chinese needs—are private) and European (most but not all) systems, where higher education funding of science, research, and development is largely part of state involvement. Research cooperation with China, in addition to the important aspect of possible threats to the competitiveness of EU companies and the success of European industrial policy, has recently acquired an additional importance—the impact it has on the European security. China's extensive and strategic cooperation with Russia, its participation in information and probably also sabotage operations, as well as its support for the Russian war economy (also in terms of technology and the substitution of Chinese for Western products in Russian supply chains) intensifies the problematic nature of cooperation with the EU. In addition to Chinese interest in technologies from modern economy sectors (genetics, medicine, robotics, artificial intelligence, electric automotive, ICT, semiconductors), or the acquisition of talent in these fields from EU member countries and soft-power activities are also an important element of Chinese activity that needs to be countered. This is again not so much about acquiring technological solutions, patents, or engineering, but about Foreign Information Manipulation & Interference (FIMI), information operations, building a positive image of China in the EU, not only within the scientific community, but also on a wider scale, shaping the views of entire societies of individual member states. China's ideas are popularized through scientific debates, conferences, seminars, student exchanges or scientific internships, and publications that present specific perspectives on issues of importance to China in the international community, which have little to do with the principle of freedom of academic debate. In the context of Sino-Russian relations, China's influence on the European security architecture (which includes cooperation with European research centers and the use of their effects for purposes contrary to the interests of Poland and the EU), it is advisable to prioritize security issues in research relations with China—even if this means a deficit and lack of access to technological solutions or scientific capabilities offered by Chinese entities.

Policy Recommendations

In this context, building on the experience of the “China Initiative,” but also taking into account the specific nature of the functioning of research and academic institutions in the EU in general and in the Member States in particular, and the somewhat different dimension of the challenges involved, it is worth considering the implementation of the following elements:

1. Including China in the set of risks for research and academic cooperation.
2. Redefining threats (not only in terms of technological solutions and patents, but also in terms of soft power and incentives for cooperation).
3. Improving the knowledge of academics and researchers about the different types of threats posed by Chinese actors, but also about China in general, how the Chinese power apparatus works and the nature of CCP policies, especially in the field of research and development.
4. Broadening the range of responses, including the establishment of “red lines” with clear restrictions.
5. Increasing the transparency of actions to reduce the possibility of accusations of biased approaches and motivations.

These basic elements could be implemented through a number of specific instruments, such as:

1. Registration by public authorities and monitoring of research contacts with Chinese entities in sectors sensitive from the point of view of national security, mainly related to high-tech or dual-use products.
2. Creating public bodies focused on strengthening the exchange of information and best practices based on public-private cooperation in research and development with China and Chinese entities.
3. Development by public bodies of guidelines for companies, research units, universities on the challenges and risks of cooperation with Chinese entities, both in terms of student exchanges, joint research, etc.
4. Restrictions by the EU and Member States on the funding of joint research projects with Chinese entities, especially in high-tech projects or dual-use products.

Bibliography

Braun Střelcová, Andrea. "Guardians of Knowledge: Why the EU's New Research Security Approach Puts European Universities in a Bind." *CHOICE*, March 7, 2024, www.chinaobservers.eu.

Hannas, William C. and Didi Kirsten Tatlow (ed.), *China's Quest for Foreign Technology*, Routledge, 2021.

Information about the Department`s Justice China Initiative and a compilation of China-Related prosecutions since 2018. February 19, 2021, www.justice.gov.

Joske, Alex. "Picking flowers, making honey." *Australian Strategic Policy Institute*, October 30, 2018, www.aspi.org.au.

Karaskova, Ivana, Filip Sebok and Veronika Blablova. "How to do trusted research: China specific guidelines for European Stakeholders," *AMO*, September 2022, www.amo.cz.

"Presidential Memorandum on United States Government-Supported Research and Development National Security Policy." *White House*, January 14, 2021, www.trumpwhitehousearchives.gov.

"Proposal for a Council recommendation on enhancing research security." *European Commission*, January 24, 2024, www.research-and-innovation.ec.europa.eu.

"Recommended practices for strengthening the security and integrity of America's science and technology research enterprise." *National Science and Technology Council*, January 2021, www.trumpwhitehousearchives.gov.

https://doi org/10 59862/k7m2x9q4r8/10

Chapter 10

The Importance of Technological Standards in Chinese Foreign Policy

BŁAŻEJ SAJDUK,
Jagiellonian University
ORCID 0000-0002-2974-8173

Abstract: This article explores the evolving role of technological standards from apolitical, technical specifications into critical instruments of geopolitical rivalry, focusing primarily on the foreign policy of the People's Republic of China. As China transitions from a technological imitator to a global leader, it increasingly leverages standard-developing organizations (SDOs) and the Belt and Road Initiative (BRI) to export its technological solutions worldwide. Through case studies of WAPI, TD-SCDMA, New IP, and 5G, the paper illustrates China's underlying motivations, including the pursuit of cyber sovereignty and the circumvention of Western licensing fees. Despite facing significant resistance from Western nations in international forums, China's de facto standardization efforts in developing nations are creating technological dependency traps. The article concludes with strategic, educational, and research recommendations for the European Union, emphasizing the need for a multidisciplinary approach to monitor and counter these initiatives to protect human rights and an open global internet.

Keywords: Technological standards, Chinese foreign policy, geopolitics, Belt and Road Initiative, standard-developing organizations

Technological standards are specifications that outline how devices should be constructed, how software should operate, and, more broadly, how technologies should function to ensure their efficiency and compatibility with other products. Modern technological standards represent one of the pivotal forces driving globalization, facilitating the seamless operation of international economic systems. Both physical and digital compatibility and interoperability are crucial elements of the global economy, enabling the efficient exchange of information and reducing production costs.

Examples of success in this area include Wi-Fi, which allows devices to connect anywhere in the world, or even such a seemingly trivial matter as the A4 paper format, which enables the use of standardized printing devices globally. Through the harmonization of standards, global networks such as the internet or radio communication can function worldwide without disruption.

Technological standards are developed by national, regional, and international standards-developing organizations (SDOs) through a process based on transparency, collaboration, and consensus.[1] Engineers, scientists, and industry representatives participate in this process, resulting in solutions that are acceptable to a wide range of stakeholders. This approach has historically led to the perception that technical standards were apolitical, existing outside of competition. However, this perspective is shifting, as the geopolitical nature of standards becomes increasingly evident.[2]

Technological standards are also referred to as soft law,[3] norms, principles, and guidelines that, while not legally binding in the traditional sense, influence the behaviors of states, international organizations, businesses, and other entities. Although standards are voluntary, their adoption brings significant technical and economic advantages to those promoting the solutions. As a result, their significance extends beyond technical aspects; they also play a strategic role in establishing market advantages and potentially geopolitical influence in the future.

Nations and corporations that dominate the standardization process can secure influence over international markets and, subsequently, legally protect

[1] Laura DeNardis, ed., *Opening Standards: The Global Politics of Interoperability* (MIT Press, 2011).

[2] Andrew D. Bishop, "Standard Power: The New Geopolitical Battle," *The National Interest, October* 7, 2015, https://nationalinterest.org/feature/standard-power-the-new-geopolitical-battle-14017.

[3] Francis Snyder, "EU, China, and Technical Standards in the Belt and Road Initiative (BRI): Extraterritoriality or Transnational Governance?" *SSRN Electronic Journal*, June 26, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4378035.

their right to benefit from licensing fees for key technologies if the standard includes patented solutions to which they hold property rights (Standard Essential Patents or SEPs). The standardization process, which involves compromise and cooperation, reflects global efforts toward integration. However, in recent years, standards have also become a field of increasingly intense geopolitical rivalry.[4] This trend is largely driven by the rising ambitions of the People's Republic of China.

China's Standardization Strategy: A Global Context

China, as a latecomer and a developing nation, has historically sought to promote its own technological standards across various new technologies. The Chinese standardization system has undergone three stages of transformation: from a phase of imitation, through a stage of catching up, to the current phase of modernization.[5] In this modern phase, technological standards are no longer merely tools for harmonizing domestic processes; they have become significant instruments of international influence.

There is increasing evidence suggesting that the world is fracturing into at least two conflicting blocs—these divisions are currently ideological but may soon extend to technological domains. One bloc consists predominantly of democratic nations led by the United States, while the other bloc comprises non-liberal-democratic states such as China and Russia, united by their opposition to the United States.

The limited success of China's efforts to establish global alternative standards to those supported by Western nations and their allies cannot serve as a reliable predictor for the future. This is because China is increasingly placing its citizens in decision-making positions within SDOs.[6] Additionally,

[4] Tim Rühlig, "The New Geopolitics of Technical Standardisation: A European Perspective," *Future Europe Journal* 3, no. 1 (2023), https://feu-journal.eu/issues/issue-3/the-new-geopolitics-of-technical-standardisation-a-european-perspective/.

[5] You-hong Yang, Ping Gao, Haimei Zhou, "Understanding the Evolution of China's Standardization Policy System," *Telecommunications Policy* 47, no. 1 (2023): 1–15, https://doi.org/10.1016/j.telpol.2022.102478.

[6] US-China Economic and Security Review Commission, *Europe-China Relations* (2023): 537–538. https://www.uscc.gov/sites/default/files/2023-11/Chapter_5_Section_1--Europe-China_Relations.pdf.

China is creating its own regulatory forums, such as the World Internet Conference—a global conference on internet issues and policies promoted by China, which challenges the vision of a global internet advocated by the Internet Corporation for Assigned Names and Numbers (ICANN).

Furthermore, China is de facto implementing its technical standards by co-financing and executing projects within the framework of the Belt and Road Initiative (BRI), which adopt Chinese solutions. The Digital Silk Road (DSR), a key component of BRI, is specifically responsible for promoting Chinese technological solutions and associated standards in the latest telecommunications technologies. This initiative plays a pivotal role in Africa, where 4G and 5G networks are being developed by Chinese companies such as Huawei and ZTE.

As part of the BRI, technical standards agreements are signed, although there is a lack of transparency regarding their detailed scope.

China's Motivations for Promoting Its Own Standards

Currently, there are several reasons why China is actively promoting its own technological standards.[7] Through these actions, China demonstrates its understanding that the ability to shape standards can effectively expand its economic, legal, political, and ideological resources.[8]

China's strategy aims to overcome what it perceives as a disadvantageous situation where it must pay excessive fees for using technologies patented by non-Chinese entities.[9] Another motivation is to pressure licensors to lower their financial demands by threatening to establish alternative solutions.

In recent years, however, the primary motivation appears to be the desire to strengthen China's international position and promote "cyber sovereignty"—a concept that reflects not only independence from the United

[7] Tim Rühlig, "Chinese Influence through Technical Standardization Power," *Journal of Contemporary China* 32, no. 139 (2023): 54–72, https://doi.org/10.1080/10670564.2022.2052439.

[8] Tim Rühlig, "Chinese Influence through Technical Standardization Power," 54–72.

[9] Michael Murphree and Dan Breznitz, "Standards, Patents and National Competitiveness," *Centre for International Governance Innovation*, no. 40, (2016): 7, https://www.cigionline.org/publications/standards-patents-and-national-competitiveness/.

States but also domestic sovereignty, which involves greater control over Chinese society and the promotion of Chinese values. This motivation is often referred to as "techno-nationalism," which can manifest with varying degrees of intensity.[10]

Examining a few examples will serve to illustrate the significance of China in the global standard-setting process.

WAPI

In 2004, China introduced the WLAN Authentication and Privacy Infrastructure (WAPI) as a mandatory national encryption standard to serve as an alternative to the international Wi-Fi standard (IEEE 802.11). Although WAPI was incompatible with international norms, Beijing anticipated that its large consumer base could be leveraged to promote this alternative technological solution. However, China's actions triggered protests within international standardization bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO). Concerns were raised, particularly regarding the lack of transparency in WAPI's development process and the potential presence of "backdoors" in the system, which posed security risks.[11]

The United States and various international organizations pressured China to collaborate with global standardization institutions to modernize existing solutions rather than introducing an alternative standard. As a result, China abandoned efforts to promote WAPI as an international standard in 2009. Notably, during the same period, South Korea attempted to advance its own standard, the Wireless Internet Platform for Interoperability (WIPI), aimed

[10] Jun Li, Yuning Liu and Cong Cao, "Competition and Collaboration: The Rise of the Chinese Standardization System," *Technological Forecasting and Social Change* 139 (2019): 10–18. https://doi.org/10.1016/j.techfore.2018.09.004; Jie Zhang and Zhimin Li, "The Impact of Information Transparency on Supply Chain Performance: A Review of the Literature," *International Journal of Information Management* 52 (2020): 102–145. https://doi.org/10.1016/j.ijinfomgt.2020.102145;Yuxi Li, Wei He and Jun Hou, "A Policy Review on the Development of Artificial Intelligence and Robotics in China: From the Perspectives of Technology, Market, and Policy," *International Journal of Information Management* 56 (2021): 102–145. https://doi.org/10.1016/j.ijinfomgt.2020.102145.

[11] Brian J. Delacey et al., Government Intervention in Standardization: The Case of WAPI (2006): 10–11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=930930.

at unifying mobile internet platforms. However, this initiative was similarly blocked by a coalition led by US technology companies.[12]

TD-SCDMA

Another example of China's attempt to promote its own standard is the Time-Division Synchronous Code-Division Multiple Access (TD-SCDMA), developed by the Chinese Academy of Telecommunications Technology (CATT). This standard was designed to support the growth of the domestic telecommunications industry and reduce the outflow of licensing fees. Backed by the Chinese government and certified by 3GPP as a variant of the 3G network standard, TD-SCDMA was deployed by China Mobile, the world's largest mobile operator by subscriber base.

Despite China's large domestic market, the effort to popularize TD-SCDMA failed internationally. The standard was deemed inefficient and inferior to existing global alternatives. Consequently, to ensure the quality of broadband mobile internet, China transitioned to Long-Term Evolution (LTE) technology, in which the European Telecommunications Standards Institute (ETSI) played a pivotal role.

New IP

New Internet Protocol (New IP) is another example of China's attempt to establish its own technical standard. Developed by Huawei, New IP was proposed as a replacement for the traditional Transmission Control Protocol/Internet Protocol (TCP/IP) architecture.[13] Work on this proposal began in 2018, and it was presented in 2019 at the International Telecommunication Union Telecommunication Standardization Advisory Group (ITU-T TSAG), a specialized United Nations (UN) agency responsible for telecommunications standards.

The ITU holds particular significance in the strategies of non-Western countries because, as part of the UN, it operates on a one-country, one-vote

[12] Heejin Lee and Sangjo Oh, "The Political Economy of Standards Setting by Newcomers: China's WAPI and South Korea's WIPI," *Telecommunications Policy* 32, no. 9–10 (2008): 662–671.

[13] Michael Safi and Patrick Wintour, "China and Huawei Propose Reinvention of the Internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.

principle, increasing the likelihood that non-democratic nations can pass their proposals. The goal of New IP was to better support modern technologies such as the Internet of Things (IoT), telemedicine, and autonomous vehicles. New IP offered deterministic routing for faster and more predictable data transmission, essential for low-latency applications. However, it also facilitated greater control over information flow, enabling censorship and surveillance and potentially contributing to internet fragmentation.[14]

A key aspect of New IP was the shift of complex network functions from endpoints to the network core, allowing for advanced data flow control. This approach aligned well with China's concept of cyber sovereignty,[15] wherein nation-states regulate information flow within their territories, contradicting the traditional vision of an open global internet. Despite Huawei's efforts to rebrand the proposal as "Future Vertical Communications Networks (FVCN)," New IP was ultimately rejected by ITU-T in December 2020 following opposition from the United States and its like -minded allies.

5G

After failing to establish its own 3G standard and playing a minor role in 4G development, Chinese authorities strategically prioritized the development of 5G technology. Recognizing 5G's potential to deliver technological and geopolitical advantages, China highlighted this priority in its strategic documents "Made in China 2025"[16] and "China Standards 2035."[17] These

[14] Julien Nocetti, *Un Internet en morceaux? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne* (Ifri, 2024).

[15] Anqi Wang, "Cyber Sovereignty at Its Boldest: A Chinese Perspective", *Ohio State Technology Law Journal* 16 (2020): 395, https://ssrn.com/abstract=4779801 or http://dx.doi.org/10.2139/ssrn.4779801.

[16] Center for Security and Emerging Technology, *Made in China 2025* (Georgetown University, 2021), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

[17] China Briefing, "China Standards 2035 Strategy: Recent Developments and Their Implications for Foreign Companies," *China Briefing*, July 12, 2022, https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/; Keiti (Huiting) Wei, "China's National Standardization Development Outline: Policy Implications and Future Directions," Institute for Future Initiatives, Securities Studies Unit, University of Tokyo 47, No. 2 (2022): 1–15, https://doi.org/10.1016/j.telpol.2022.102478.

documents position 5G as a key technology where China aims to achieve global leadership.[18]

5G technology not only supports faster data transmission but also enables advancements in areas such as IoT, autonomous vehicles, smart cities, and Industry 4.0. Chinese companies currently account for approximately 35% of contributions to 5G standards established by the 3rd Generation Partnership Project (3GPP), surpassing contributions from Europe (32%) and the United States (16%).[19]

While China has achieved technological self-reliance in 5G, US security concerns, exemplified by initiatives like the Clean Network,[20] have led American allies in Europe and Asia to seek ways to limit the use of Huawei equipment.[21]

Conclusion and Recommendations

The examples mentioned previously indicate that China still possesses limited ability to impose specific international technological standards through SDOs.[22] In the cases described, Chinese initiatives were blocked, making the formal adoption of standards promoted by Chinese enterprises largely ineffective. In response to the strong resistance from Western nations and other like-minded countries, China employs alternative tools to build its technological sphere of influence, particularly through de facto standardization, implementing technological solutions without formal approval by SDOs.

The Belt and Road Initiative (BRI) plays a pivotal role in this strategy, serving as a means to export Chinese technologies and standards to

[18] Elsa Kania, "China's Play for Global 5G Dominance: Standards and the Digital Silk Road," *The Strategist*, June 27, 2018, https://www.aspistrategist.org.au/chinas-play-for-global-5g-dominance-standards-and-the-digital-silk-road/.

[19] Tim Nicholas Rühlig and Tobias ten Brink, "The Externalization of China's Technical Standardization Approach," *Development and Change* 52, no. 5 (2021): 1207, https://doi.org/10.1111/dech.12685.

[20] U.S. Department of State, "The Clean Network," *U.S. Department of State*, accessed June 14, 2024, https://2017-2021.state.gov/the-clean-network/index.html.

[21] Zhan Zhang, "Technology and Geopolitics: The Social Construction of Huawei's 5G Controversy in Europe," *Global Media and Communication* 20, no. 2 (2024): 217–235, https://doi.org/10.1177/17427665241251448.

[22] Sorina Teleanu, *The Geopolitics of Digital Standards: China's Role in Standard-Setting Organisations* (DiploFoundation, 2021), https://www.diplomacy.edu/wp-content/uploads/2021/12/Geopolitics-of-Digital-Standards-Dec-2021.pdf.

other countries, thereby creating potential technological "dependency traps."[23] These traps operate such that adopting one Chinese technological solution necessitates using other compatible solutions. Chinese activity is particularly notable in Africa[24] and Southeast Asia,[25] where the adoption of Chinese technological standards will significantly impact the future trajectory of industrial and trade development on these continents. For example, adopting Chinese standards in telecommunications infrastructure or railway systems not only ensures compatibility with other Chinese technologies but also requires adherence to Chinese norms and the training of personnel capable of maintaining and operating these systems.

Huawei, in particular, leverages its resources to build relationships with universities in African countries. Through these efforts, Huawei not only promotes its own equipment and standards but also offers certifications as alternatives to those provided by Western entities.[26] This approach grants Chinese enterprises a structural and long-term advantage.

A growing concern is China's capability to deploy network monitoring solutions that control and filter both incoming and outgoing content within China's cyberspace, known as the "Great Firewall of China." Moreover, these solutions, along with the underlying philosophy of maintaining social stability at the expense of individual freedoms, are often seen as desirable capabilities in non-democratic states. A notable example is Cambodia's replication of China-style firewall capabilities.[27]

[23] Tim Rühlig, "China's Technical Standardization Power – A Challenge for NATO?" *International Journal* 78, no. 4 (2023): 625–633, https://www.swp-berlin.org/10.18449/2019C29/.

[24] Juan Vázquez Rojo, "China's Technological Footprint in Africa: A Patent Network Analysis," *South African Journal of Business Management* 55, no. 1 (2024), https://sajbm.org/index.php/sajbm/article/view/4331/2854.

[25] ARTICLE 19, *Digital Silk Road: Advancing China's Model of Digital Authoritarianism*, March 2024, https://www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf.

[26] Matthias Bauer and Nadine Godehardt, "Learning along the Digital Silk Road? Technology Transfer, Power, and Politics in China's ICT Engagements in Algeria and Egypt," *The Information Society* 40, no. 2 (2024): 146–147, https://doi.org/10.1080/01972243.2024.2317060.

[27] ARTICLE 19, *Digital Silk Road: Advancing China's Model of Digital Authoritarianism*, (2024): 31–37, https://www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf.

Strategic Recommendations

Protecting values and principles requires EU member states to focus not only on content regulation but also on the hardware layer and the technological standards underpinning it. Technological standards will undoubtedly remain a permanent aspect of US-China competition, especially in the realm of cutting-edge technologies. The optimal strategy for EU Member States in this conflict is to closely monitor Chinese activities within SDOs that aim to establish alternative solutions, particularly in the context of protecting an open internet and human rights.

A multidisciplinary approach is essential for analyzing these processes, as they cannot be fully addressed through technical, legal, or international security expertise alone.

Policy Recommendations

Protecting values and principles requires EU Member States to focus not only on content regulation but also on the hardware layer and the technological standards underpinning it. Technological standards will undoubtedly remain a permanent aspect of US-China competition, especially in the realm of cutting-edge technologies. The optimal strategy for EU Member States in this conflict is to closely monitor Chinese activities within SDOs that aim to establish alternative solutions, particularly in the context of protecting an open internet and human rights.

A multidisciplinary approach is essential for analyzing these processes, as they cannot be fully addressed through technical, legal, or international security expertise alone.

Research and Educational Recommendations

1. Research:

- Increase financial support for research programs addressing the potential risks of implementing standards that challenge existing solutions, especially in the field of telecommunications technology, which underpins future knowledge-based economies.

2. Education:

- Integrate the (geo-)political dimension of standardization policy into technical and legal curricula.
- Expand International Relations and International Security Studies programs to include content that explains the technical aspects of standardization (particularly for emerging technologies).
- Incorporate the legal-procedural aspects of the standard-setting process into existing curricula to provide a comprehensive understanding of how technical standards are established and enforced.

Bibliography

Bauer, Matthias and Nadine Godehardt. "Learning along the Digital Silk Road? Technology Transfer, Power, and Politics in China's ICT Engagements in Algeria and Egypt." *The Information Society* 40, no. 2 (2024): 163–176. https://doi.org/10.1080/01972243.2024.2317060.

Bishop, Andrew D. "Standard Power: The New Geopolitical Battle." *The National Interest*. October 7, 2015. https://nationalinterest.org/feature/standard-power-the-new-geopolitical-battle-14017.

Center for Security and Emerging Technology. Made in China 2025. Washington, D.C.: Georgetown University, 2021. https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

"China Standards 2035 Strategy: Recent Developments and Their Implications for Foreign Companies." *China Briefing*, July 12, 2022. https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/.

DeNardis, Laura, ed. *Opening Standards: The Global Politics of Interoperability*. MIT Press, 2011.

Delacey, Brian J., et al. *Government Intervention in Standardization: The Case of WAPI.* 2006. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=930930.

Kania, Elsa. "China's Play for Global 5G Dominance: Standards and the Digital Silk Road." *The Strategist*, June 27, 2018. https://www.aspistrategist.org.au/chinas-play-for-global-5g-dominance-standards-and-the-digital-silk-road/.

Lee, Heejin and Sangjo Oh. "The Political Economy of Standards Setting by Newcomers: China's WAPI and South Korea's WIPI." *Telecommunications Policy* 32, no. 9–10 (October–November 2008): 662–71.

Li, Jun, Yuning Liu and Cong Cao. "Competition and Collaboration: The Rise of the Chinese Standardization System." *Technological Forecasting and Social Change* 139 (2019): 10–18. https://doi.org/10.1016/j.techfore.2018.09.004.

Motolani Agbebi. "China's Digital Silk Road and Africa's Technological Future." *Council on Foreign Relations*, February 1, 2022. https://www.cfr.org/blog/chinas-digital-silk-road-and-africas-technological-future.

Murphree, Michael and Dan Breznitz. *Standards, Patents and National Competitiveness,* no. 40, (2016): 7. https://www.cigionline.org/static/documents/gcig_no.40web.pdf.

Nocetti, Julien. *Un Internet en morceaux? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne*. Ifri, 2024.

Rühlig, Tim. "China's Technical Standardization Power—A Challenge for NATO?" *International Journal* 78, no. 4 (2023): 625–633. https://journals.sagepub.com/doi/10.1177/00207020231217117.

Rühlig, Tim. "The New Geopolitics of Technical Standardisation: A European Perspective." *Future Europe Journal* 3, no.1 (2023). https://feu-journal.eu/issues/issue-3/the-new-geopolitics-of-technical-standardisation-a-european-perspective/.

Rühlig, Tim Nicholas and Tobias ten Brink. "The Externalization of China's Technical Standardization Approach." *Development and Change* 52, no. 5 (2021): 1196–1221. https://doi.org/10.1111/dech.12685.

Safi, Michael and Patrick Wintour. "China and Huawei Propose Reinvention of the Internet." *Financial Times*, March 27, 2020. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.

Snyder, Francis. "EU, China, and Technical Standards in the Belt and Road Initiative (BRI): Extraterritoriality or Transnational Governance?" *SSRN Electronic Journal*, June 26, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4378035.

Teleanu, Sorina. *The Geopolitics of Digital Standards: China's Role in Standard-Setting Organisations*. DiploFoundation, 2021. https://www.diplomacy.edu/resource/report-the-geopolitics-of-digital-standards-chinas-role-in-standard-setting-organisations/

US-China Economic and Security Review Commission. *Europe-China Relations*. 2023: 537–538. https://www.uscc.gov/sites/default/files/2023-11/Chapter_5_Section_1--Europe-China_Relations.pdf.

U.S. Department of State. "The Clean Network." *U.S. Department of State*. Accessed November 20, 2024. https://2017-2021.state.gov/the-clean-network/index.html.

Vázquez Rojo, Juan. "China's Technological Footprint in Africa: A Patent Network Analysis." *South African Journal of Business Management* 55, no. 1, (2024). https://sajbm.org/index.php/sajbm/article/view/4331/2854.

Xu, Young. "Deconstructing the Great Firewall of China." *ThousandEyes*. March 8, 2016. https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.

Yang, You-hong, Ping Gao and Haimei Zhou. "Understanding the Evolution of China's Standardization Policy System." *Telecommunications Policy* 47, no. 1 (2023): 1–15. https://doi.org/10.1016/j.telpol.2022.102478.

Zhang, Zhan. "Technology and Geopolitics: The Social Construction of Huawei's 5G Controversy in Europe." *Global Media and Communication* 20, no. 2 (2024): 217–235. https://doi.org/10.1177/17427665241251448.

https://doi org/10 59862/k7m2x9q4r8/11

Chapter 11

Russian Influence Activities and Espionage in the Estonian Academic Environment: The Case of Viacheslav Morozov, a Russian GRU Spy at the University of Tartu[1]

VLADIMIR SAZONOV
University of Tartu
ORCID ID 0000-0001-9738-1329

Abstract: The current chapter is dedicated to the case of Viacheslav Morozov, a Russian GRU spy who worked at the University of Tartu for several years. This chapter provides an overview of Morozov's academic activity and how he disseminated Marxist ideas and pro-Kremlin narratives through scientific publications, lectures, conferences, and scientific-popular works.

Keywords: Russia, Viacheslav Morozov, University of Tartu, spy, GRU, academic espionage, information influence activity, pro-Kremlin narratives, Russophobia, Marxism

Introduction

Over the past two decades, we have seen an increase in Russian influence activities (among them disinformation campaigns, espionage) and other hybrid warfare activities around the world—especially since 2014, when Russia first attacked Ukraine[2] and which intensified after February 24, 2022, when Russia launched a full-scale military invasion of Ukraine.

[1] Research-Professor at the Estonian Military Academy and Associate Professor at the University of Tartu, sazonov@ut.ee.

[2] See more: Vladimir Sazonov, Erkki Koort, Priit Heinsoo and Kadri Paas, *Introduction of Hybrid Threats of Internal Security* (Estonian Academy of Security Sciences, 2020); Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Rand Corporation, 2017).

One of the tools of Russian hybrid warfare is espionage, which the Kremlin has actively used. There are many cases of Russian spies, agents of influence, and pro-Russian activists in the West across all spheres, such as economics, politics, security, the military, society, culture, as well as science and education.

The current overview chapter is dedicated to one recent case of Russian espionage in the Estonian academic environment—the case of Viacheslav Morozov. Morozov was Professor of International Political Theory at the Johan Skytte Institute of Political Studies at the University of Tartu where he worked for thirteen years, and where, in addition to his academic work as a scientist and university lecturer, he was involved in espionage. In its 2023–2024 annual report, Estonia's Internal Security Agency (KAPO) noted Morozov's intelligence activities in Estonia:

"I*n January 2024, KAPO apprehended Viacheslav Morozov, a professor at the University of Tartu, suspected of engaging in and supporting intelligence activities against Estonia. According to preliminary information, Morozov co-operated with Russian special services for years*."[3]

In June 2024, Harju County Court (Estonia) found Morozov guilty of activities against the Republic of Estonia and he was sentenced to six years and three months in prison.[4] Chief State Prosecutor Taavi Pern said that the court's verdict confirmed that Morozov had cooperated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) for a long time, stressing that Morozov was assigned by the Russian special services to collect information on Estonia's domestic, defense, and security policy, as well as its people and infrastructure.[5]

Taking all the above into consideration, I will qualitatively analyze some of Morozov's statements and ideas about Russia and its policies, etc.[6] I will focus

[3] See: *Estonian Internal Security Service Annual Review 2023–2024*, 20, accessed July 21, 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf

[4] "Venelaste jaoks luuranud Tartu ülikooli professor Vjatšeslav Morozov saadeti kuueks aastaks vangi," Reporter.ee, June 18, 2024, https://reporter.kanal2.ee/8043436/venelaste-jaoks-luuranud-tartu-ulikooli-professor-vjatseslav-morozov-saadeti-kuueks-aastaks-vangi.

[5] "Kohus mõistis Viatcheslav Morozov süüdi luuretegevuses," *Kaitsepolitseiamet*, June 18, 2024, https://kapo.ee/et/content/kohus-moistis-viatcheslav-morozov-suudi-luuretegevuses/.

[6] Udo Kuckartz, *Qualitative Text Analysis: A Guide to Methods. Practice & Using Software* (Sage Publications 2014).

on some of Morozov's works published in academic and scientific-popular texts or presented at conferences and lectures. According to *Estonian Internal Security Service*, Morozov was working for the GRU[7] and seems that he probably also completed other tasks, among them promoting (mostly hidden) pro-Kremlin narratives, e.g., narrative about Russophobia.[8]

Morozov as a GRU Spy and His Potential Tasks

Before proceeding to an analysis of Morozov's[9] works and academic activity, a few key aspects must be explained.

Firstly, the kind of assignments Morozov could have received from the GRU and other Russian special intelligence services or at least define in general terms the scope of his espionage activities in Tartu.

Secondly, as I don't have access to Morozov's classified case files, we can only speculate on the kind of espionage he was engaged in. The scant data on this can be gleaned from statements by the prosecutor's office and KAPO, as well as from security experts who have analyzed this case. For example, Arnold Sinisalu, former director of KAPO, said in an interview on January 21, 2024, that Russian intelligence is interested in Estonia and that hundreds of people are engaged in intelligence activities against Estonia.[10] From open sources we can find information about the potential tasks of Morozov.

[7] Estonian Internal Security Service Annual Review 2023–2024, 20, accessed July 21, 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf

[8] Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," Vabariik, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/. See also the interview with Arnold Sinisalu, former Chief of the Estonian Internal Security Service, who highlighted: "…it cannot be ruled out that Morozov had specific tasks to develop Russian propaganda activities in the course of his research. After all, researchers are allowed more freedom; they can discuss both sides of an argument.“ Aaspõllu, Huko. "Sinisalu: Venemaal tegeleb Eesti-vastase luuretegevusega sadu inimesi." Err, January 21, 2024, https://www.err.ee/1609227084/sinisalu-venemaal-tegeleb-eesti-vastase-luuretegevusega-sadu-inimesi

[9] For a better understanding of the GRU spy Viacheslav Morozov, who was active at the University of Tartu for almost fourteen years (2010—January 2024), and a brief overview about his life, education, and career, please see his academic CV on the "Estonian Research Information System," https://www.etis.ee/Portal/Persons/Display/0d15338c-29e1-4ac1-bd17-cde2f2d46466/eng.

[10] Huko Aaspõllu, "Sinisalu: Venemaal tegeleb Eesti-vastase luuretegevusega sadu inimesi," Err, January 21, 2024, https://www.err.ee/1609227084/sinisalu-venemaal-tegeleb-eesti-vastase-luuretegevusega-sadu-inimesi.

Although this information is very brief, we can assume that he was very active, especially if we look at his academic work and scientific activity in Estonia and around the Western world.

Estonian security expert Erkki Koort commented: "*Morozov's case clearly shows that Russian military intelligence is not only interested in gathering military information. He was working with a university that does have contacts with military intelligence targets. The university carries out research commissioned by the state, which enables a spy to understand the interests of state institutions, and the presentation of the research to the leadership gives an idea of who holds what position in the ministry or what opinions different conclusions generate. Similarly, joining a spy group allows the spy to steer the group's research or study in the desired direction, leaving out things they want to avoid.*"[11]

We don't know in detail what tasks Morozov was given by the GRU and how he collected and passed on data, but KAPO and the Estonian Prosecutor's Office have given general information of what Morozov did while working at the University of Tartu. According to this information, Morozov was recruited by Russian intelligence in the early 1990s while he was studying at a university in Russia.[12]

The GRU instructed him to become more active when he moved to Estonia. Morozov probably provided the special services of Russia with information on the political situation and elections in Estonia, alliance relations, and social integration. This was information to which he had access, both because of his position as a researcher and because it was publicly available, which could be used by Russia to threaten Estonia.[13]

Koort supposed rightly that today's students at university would be tomorrow's decision-makers, and information about their connections and perso-

[11] Erkki Koort, "Venemaa sõjaväeluure spioon Tartus ja Eesti sihtmärgid Venemaal," *Postimees*, June 21, 2024, https://arvamus.postimees.ee/8045133/erkki-koort-venemaa-sojavaeluure-spioon-tartus-ja-eesti-sihtmargid-venemaal.

[12] Andres Einmann, "GRU värbas Eestis luuranud professori juba 1990. aastate alguses," *Postimees*, June 19, 2024, https://www.postimees.ee/8043515/gru-varbas-eestis-luuranud-professori-juba-1990-aastate-alguses. See also *Estonian Internal Security Service Annual Review 2024–2025*, 30, accessed 29 December 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf

[13] "Kohus mõistis Viatcheslav Morozov süüdi luuretegevuses," *Kaitsepolitseiamet*, June 18, 2024, https://kapo.ee/et/content/kohus-moistis-viatcheslav-morozov-suudi-luuretegevuses/.

nal characteristics could be the information needed in the future to decide who to recruit by the GRU, FSB, or other Russian intelligence services.[14]

Japanese political scientist Sanshiro Hosaka, who works and studies at the University of Tartu, also presented his suspicions about Morozov, whom Hosaka knew as a colleague: "*Morozov was convicted only for gathering, analyzing, and passing information to Russian intelligence. I presume Morozov denied any malicious intent in his activities related to academia.*"[15] *But Hosaka showed clearly how Morozov promoted pro-Russian ideas and narratives at the University of Tartu. Hosaka also emphasized that "when Russian intelligence disseminated narratives on possible Russia-Europe cooperation in ecology and environment in 2021, coincidentally, he (Morozov) gave a series of lectures on Russian environmental policies.*"[16]

Morozov's Activities at the University of Tartu and in the Academic World

In the following chapter I will give a brief overview of some examples of Morozov's academic activities, from which it appears that Morozov's possible ambition was, under the guise of academic and teaching activities, to collect data about colleagues, to influence students and public opinion with his ideas, to infiltrate various scientific councils and networks, and to collect information on the political situation and important people in Estonian society, and so on.

I dare to suppose that former professor Viacheslav Morozov could have tried to recruit new agents for the GRU, both in in Estonia and abroad—or at least it should be not excluded.

Morozov's Activity in the Academic Environment of the University of Tartu

As a university teacher, Morozov has been very active and prolific in publishing scientific articles in prominent scientific journals such as *Internatio-*

[14] Ibid.

[15] Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

[16] Ibid.

nal Theory, International Relations, Journal of International Relations and Development, etc., as well as popular science reviews, and he has often appeared in Estonian media both in Russian and Estonian.

He was also very active in the field of networking of scientists, and as a teacher he gave many lectures and seminars, supervised students' scientific works at all levels, from bachelor's to doctoral level, and was a member of various councils at the university.

Morozov activities in CEURUS

One important scientific center at the University of Tartu in which Morozov was actively involved is the Centre for Eurasian and Russian Studies (CEURUS),[17] where he was academic director from 2020 until January 2024.

In May 2013, Morozov published a comment in the newspaper of the University of Tartu, where he wrote: "*In March 2011, when the Centre for EU and Russian Studies Ceurus was one of the first to receive a grant of 1.6 millions euros from the newly established Development Fund of the University of Tartu. … The rector emphasized the great potential of the Centre due to its geographical and historical position.*"[18]

Other information about the activities of Viacheslav Morozov in CEURUS can be found by searching for his name on CEURUS' homepage.[19]

Pro-Russian Activities at Conferences and Seminars

Morozov actively participated in conferences in Tartu and across the world, and organized seminars and conferences at the University of Tartu himself.

For several years Morozov was a chairman of the program committee and main organizer of yearly Eastern European and Russian Studies conferences

[17] The Centre for Eurasian and Russian Studies is an interdisciplinary center for research and teaching at the University of Tartu. The idea of creating of CEURUS is establishing as a bridge for scholars, students and members of the public interested in the past, present and future of the Eurasian space, accessed November 2, 2024, https://ceurus.ut.ee.

[18] Viacheslav Morozov, "Ceurus meelitab Tartusse tunnustatud teadlasiz," *Universtas Tartuensis* 5, May 2013, https://www.ajakiri.ut.ee/artikkel/947.

[19] "The Centre for Eurasian and Russian Studies (CEURUS)," University of Tartu, accessed November 19, 2024, https://ceurus.ut.ee/?s=Morozov&x=0&y=0.

in Tartu.[20] These conferences organized by Morozov and other scholars were attended by, among others, very well-known scholars, among them historians, political scientists, sociologists, and others from Europe, Russia, the United States, and many other places, particularly Asia.

How Morozov used conferences and seminars as a platform remains to be seen. Here are a few examples. For example, Sanshiro Hosaka wrote in 2024 that Morozov "was invited to the Lennart Meri conference three years ago, along with other academics in the country, as part of efforts to bridge this practitioner-academic chasm,"[21] although it is a matter for discussion how he could leverage this new platform for his intelligence activities.

Hosaka also highlighted that in June 2022 at the Eastern European and Russian Studies conference in Tartu, Morozov chaired a round table on "A Future of Russian Studies,“ to which he invited his good friends and colleagues with neo-Marxist views and Morozov tried to show that the Western world is Russophobic towards Russia and Morozov argued that academic interaction with Russian research institutions should continue. At which point Hosaka asked him: "*How can we talk about academic exchanges with Russian 'educational' institutions if many of them are housing FSB seconded officers?*" Morozov interrupted Hosaka's question and didn't answer. There are also other examples or cases where Morozov's behavior at conferences seemed strange.[22]

Morozov as Grant Holder

Viacheslav Morozov was also successful in writing and receiving grants in Estonia and abroad. I will present just a few examples here.

Morozov was holder of several scientific grants from Estonian and Eu-

[20] Fifth Annual Tartu Conference, "Post-Socialist (dis)Orders," accessed November 15, 2024, https://sisu.ut.ee/tartuconference/fifth-annual-tartu-conference-2021/.

[21] Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

[22] On May 31, 2021, I took part in a roundtable at the University of Tartu entitled: "The rise of populism and information warfare – the influence of Russian strategic narratives on the Global Knowledge Warfare," at which Morozov was in the audience. Morozov commented with skepticism when the presenters criticized Russian aggressive imperialism. See "Roundtables mark the beginning of this year's Tartu Conference on Russian and East European Studies," University of Tartu, May 18, 2021, https://skytte.ut.ee/en/content/roundtables-mark-beginning-years-tartu-conference-russian-and-east-european-studies.

ropean foundations. The last scientific project of Morozov was entitled "National identity and Estonian-Russian relations: a longitudinal study of elite and mass discourses." Morozov received this scientific project from the Estonian Research Council (with a considerable amount of financial sources €691,900 for three years 2021–2024.[23]

Prior to that, Morozov was grant holder of other projects, for example: "When every act is war: Post-Crimea conflict dynamics and Russian foreign policy" (2020–2024) which he received from the Research Council of Norway,[24] and "Decision-making in domestic and foreign policy processes of the Russian Federation" (June 1, 2022, to May 31, 2023) which Morozov received from the Ministry of Foreign Affairs of Estonia[25] and several others.

Morozov's Lectures at the University of Tartu and Opinions about His Teaching

There can be no doubt that, as university teacher, Morozov could influence many students who studied in Tartu from all over the world and probably tried to create a network for the GRU, and collect information which he gave to the GRU during his very frequent visits to Russia. Morozov also used often ultra-leftist and Marxist theories and promoted these views in his works, other texts, and lectures.[26]

A student who attended Morozov's lectures in 2022–2023 explained that Viacheslav Morozov emphasized the ills of Russia, and in this student's opinion he analyzed Russia objectively, was able to explain to students how the Russian economy worked, and often spoke about the corruption

[23] See more about this grant at: https://www.etis.ee/Portal/Projects/Display/df35aa0f-1010-4884-b7aa-b423f8f09026; see more about scientific biography of Morozov where all grants received from the Estonian Research Council or other European foundations are listed, accessed on November 17, 2024, https://www.etis.ee/Portal/Projects/Display/df35aa0f-1010-4884-b7aa-b423f8f09026.

[24] "Estonian Research Information System," accessed on November 21, 2024, https://www.etis.ee/Portal/Projects/Display/40a4b3e8-49fb-4b5f-80c0-ef9d58e48668.

[25] "Estonian Research Information System," accessed on November 1, 2024, https://www.etis.ee/Portal/Projects/Display/46389e4a-6e65-4a71-b2c0-2a4dc447a4e2.

[26] Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

thriving in Russia. However, according to several students, on the topic of Russia's military aggression against Ukraine in 2022, one listener of his lectures recalled that no analysis on this topic was given at Morozov's lectures. According to other students, Morozov was not in a hurry to criticize and speak negatively about the actions of Putin's regime.[27] But there are also other students' opinion who highlight that Morozov was critical toward Russia and Putin's regime.[28]

Morozov as an Opinion Leader and Author of Academic Works

In this last chapter I will present analysis of some of Morozov's academic and non-academic works as examples chosen to show what kind of ideas he presented and disseminated in the academic world in Estonia and as an analyst in reports whose target audience were politicians, decision-makers, and think-tank analysts, as well as more broadly in the West and as an opinion leader in Estonia who wrote for both an Estonian and Russian audience.[29]

Let us take a closer look at what Morozov's views were as an author and opinion leader who published a lot in Estonian, English, and Russian, and even in the *Riigikogu Toimetised* ("The Proceedings of the Riigikogu"— the parliament of Estonia).[30]

As Erkki Koort rightly said: "*In the Morozov case, what came out of the public debate was that he did not support Putin's direction at all and was talking a completely different story from the Kremlin regime. This is the only way to spy successfully, because if he had told the Kremlin's version, he would*

[27] Peeter Espak, "Venemeelne ja läänevastane marksist Vjatšeslav Morozov," *Err.*, January 20, 2024, https://www.err.ee/1609228107/peeter-espak-venemeelne-ja-laanevastane-marksist-vjatseslav-morozov.

[28] Л.-Э. Ломп, "Студенты: задержанный по подозрению в шпионаже против Эстонии преподаватель относился к России скорее критически," *Rus.Postimees*, January 16, 2024, https://rus.postimees.ee/7939521/studenty-zaderzhannyy-po-podozreniyu-v-shpionazhe-protiv-estonii-prepodavatel-otnosilsya-k-rossii-skoree-kriticheski.

[29] There were dozens of these broadcasts and listening to a few of them I couldn't yet draw any firm conclusions, but Morozov's idea was apparently to get a number of scientists from Russia, including his wife and colleague Elena Pavlova, on Russian-language radio. See more at the Centre for Eurasian and Russian Studies, University of Tartu, https://ceurus.ut.ee/viacheslav-morozov-to-co-host-a-radio-show-on-estonian-public-broadcasting/.

[30] Viacheslav Morozov et al. "Vene rehepapp, Kremli välispoliitika populaarsus ja de facto riigid," *Riigikogu Toimetised Riigikogu Toimetised* 40 (2019): 75–85.

not have had the opportunity to work for long and build trusting relationships."[31]

It would be naive to think that a Russian spy would openly disseminate the Kremlin's strategic narratives and propaganda messages, but I argue that we still can find some ideas in Morozov's texts that directly or indirectly support a pro-Kremlin agenda and could be used to justify Russian imperialism and military aggression.

Viacheslav Morozov often published his articles and views in scientific -popular outlets and the most important Estonian newspapers in Estonian and Russian languages, and he also appeared on television and radio.[32]

In 2009, one year prior to his position at the University of Tartu, Morozov published an article[33] in the Estonian magazine *Diplomaatia* entitled "Russia and the West: playing by the rules?" that deals with questions of politics and security, where he used a pro-Kremlin propaganda statement that Russia is not threat to the West: "*Russia does not pose the slightest radical threat to the established normative order of Western dominance. Far from being a revolutionary force, it is waging a positional war for the interpretation of norms and values, while holding them to be universally valid.*"[34] The idea that Russia is peaceful and does not pose a threat for its neighbors has been promoted by Putin's regime in pro-Kremlin discourse for decades, and, for example, more recently by Dmitri Peskov, press secretary of the Russian dictator.[35]

[31] Erkki Koort, "Venemaa sõjaväeluure spioon Tartus ja Eesti sihtmärgid Venemaal,“ Postimees, June 21, 2024, https://arvamus.postimees.ee/8045133/erkki-koort-venemaa-sojavaeluure-spioon-tartus-ja-eesti-sihtmargid-venemaal.

[32] See, for example, Radio 4, https://r4.err.ee/1608595918/sosedi, May 23, 2022. It is worth mentioning that in 2021–2022, Viacheslav Morozov co-hosted together several radio shows with Evgeniya Savina at the Estonian Public Broadcasting in a Russian-language radio Estonian Radio 4 program called "Соседи" (Neighbors). Twice a month, this program discussed various issues and developments in the post-Soviet space in popular science perspective with several invited guests.

[33] Viacheslav Morozov, "Russia and the West: playing by the rules? \ Venemaa ja Lääs: mäng reeglite järgi?" *Diplomaatia* 74/75, (November 2009), https://diplomaatia.ee/venemaa-ja-laas-mang-reeglite-jargi/.

[34] Ibid.

[35] See: Ю.Катенова, "Песков: Россия не угрожает никому в Европе," *Парламентская газете*, April 26, 2024, https://www.pnp.ru/politics/peskov-rossiya-ne-predstavlyaet-ugrozy-ni-dlya-kogo-v-evrope.html; "Россия не представляет угрозы для Запада": *SIPRI подсчитал военные расходы стран. Военное обозрение*, June 1, 2024, https://topwar.ru/243580-rossija-ne-predstavljaet-ugrozy-dlja-zapada-sipri-podschital-voennye-rashody-stran.html.

As Peeter Espak showed in his analysis,[36] Morozov explains in his article published in 2009 in *Diplomaatia* that this Western-created world order is probably not the only option, and the world needs a "Pluriverse" instead of a "universe." Morozov argues that Putin's multipolar world might not be such a bad thing, and that the West should instead try to make friends with this image.[37]

On March 29, 2021, in an interview in Estonian daily newspaper *Eesti Päevaleht*, Morozov also promoted ideas of the Russian political elite or Russian so-called regime opponents, who are against Putin but at same time often shows their sympathy to Russian imperialism and even Russia's aggressive war in Ukraine.[38] Among others, Morozov declares: "*I don't think Russia has any values that are very different from the West. It is perhaps a little more conservative, but you will also find it in Europe, including in this country, those who share its views on gay marriage or women's rights, for example. He has a more traditional approach.*"[39]

Here, Morozov again defends Russia, but does so not in a directly offensive way like the simplistic Russian propaganda channels, but in a more cunning way similar to many of the more subtle pro-Kremlin channels that disseminate Russian propaganda. In Morozov's discussion with the journalist, we can read that Morozov's idea is that Russia would get along well with the West if the West, including the US, would accept Russia (meaning accepting Russia's imperialist goals and aggressive politics): *"Russia, however, clearly feels insecure and believes that the West is undermining its security by interfering in Ukraine, Georgia, and Moldova*." Morozov also brought up the idea, promoted by the Kremlin and Putin himself, that the West does not see Russia as an equal and therefore Russia is forced to take action. To the jo-

[36] Peeter Espak, "Venemeelne ja läänevastane marksist Vjatšeslav Morozov," *Err*, January 1, 2024, https://www.err.ee/1609228107/peeter-espak-venemeelne-ja-laanevastane-marksist-vjatseslav-morozov.

[37] Ibid. See about Putin's multipolar ideas and Primakov's doctrine. Also see Putin's statement that the world has become multipolar: "Путин заявил о ставшем реальностью многополярном мире," *РБК*, July 4, 2024, https://www.rbc.ru/rbcfreenews/66865a079a794793ab095cb3.

[38] Krister Paris, "Vjatšeslav Morozov: ebakinda ja haavatavana tunneb end mitte niivõrd lääs kui hoopis Venemaa," *Eesti Päevahaleht*, March 29, 2021, https://epl.delfi.ee/artikkel/92983781/intervjuu-vjatseslav-morozov-ebakinda-ja-haavatavana-tunneb-end-mitte-niivord-laas-kui-hoopis-venemaa.

[39] Ibid.

urnalist's question: "*But if we now look at Russia in the Moscow-Washington -Beijing triangle, what role does it play there? Washington is verbally attacking both at the moment, but perhaps in the long term, Russia and the US can still put their backs together? Would Russia take up the offer?*" Morozov replied: "I*t would be more likely to side with China in the current circumstances. True, if the West accepted him and treated him as an equal, the West would be the natural choice.*"[40]

On March 4, 2022, a week after Russian military aggression against Ukraine, Morozov's opinion was published in the Russian-language portal *Estonian Public Broadcasting* entitled "The war with Ukraine ended the history of post-Soviet Russia"[41] where Morozov declared: "*These days, we are all facing many moral dilemmas and personal tragedies caused by war. Undoubtedly, the people of Ukraine, who have faced brutal military aggression, are the hardest hit. We have no idea yet of the full extent of the losses. It is clear, however, that the number of dead and wounded will continue to grow*." Although he mentioned Russian military aggression against Ukraine war and showed sympathy toward Ukraine and Ukrainian people, Morozov also showed deep concerns for Russians and Russia:

"…*Russians are also having a hard time. .... The economic devastation created by sanctions and military spending is already beginning to affect the lives of ordinary people. As families learn of the deaths of their sons, the scale of war losses will be realized*." [42]

Two weeks later on March 18, 2022, Morozov answered journalist's questions in a regular program of the Rus.Postimees portal dedicated to the military situation in Ukraine and the international political situation. Morozov commented on the military situation and Russia's war in Ukraine, answered questions related to the high risk of a big war in Europe, and spoke about the

[40] Krister Paris, "Vjatšeslav Morozov: ebakinda ja haavatavana tunneb end mitte niivõrd lääs kui hoopis Venemaa," *Eesti Päevahaleht*, March 29, 2021, https://epl.delfi.ee/artikkel/92983781/intervjuu-vjatseslav-morozov-ebakinda-ja-haavatavana-tunneb-end-mitte-niivord-laas-kui-hoopis-venemaa.

[41] В.Морозов, "Война с Украиной положила конец истории постсоветской России," *Rus. Err*, March 4, 2022, https://rus.err.ee/1608520970/vjacheslav-morozov-vojna-s-ukrainoj-polozhila-konec-istorii-postsovetskoj-rossii.

[42] Ibid.

signals sent by US President Joe Biden to the Russian military leaders and Putin, etc.[43]

According to Morozov: "*On the basis of intelligence data, as well as any objective data in general, no one can make an accurate conclusion about whether there will be a war and what its probability is. So, I assume that Emmanuel Macron was just analyzing the course of his conversations with Vladimir Putin, the course of his contacts with him, which have been quite intense throughout this crisis. Macron, I assume, has studied very well the signals that Putin is sending during these talks, and I think that's what has been the decisive factor in Macron's assessment, because he realizes that Vladimir Putin is ready to go quite far, ready to go for further escalation. That's obvious. And it's also evident from what's happening in Ukraine, what's happening in Russia, how the Russian elites are behaving. All this shows that the possibility of a big war exists and it is quite high.*"[44]

We cannot see that Morozov promoted pro-Russian narratives here. However, in response to a journalist's comment that, according to the Kremlin, one of Russia's goals in launching a full-scale military attack on Ukraine is to "denazify" the country, Morozov said that Moscow's main allies in Europe in recent years have been alt-right parties that have assiduously defended the Kremlin's foreign policy.

Morozov answered in the following way: "*After a certain point—not even now, but about 2–3 years ago—there was a turning point where Putin stopped being interested in the West. That's why he so blatantly misinformed his colleagues, that's why he so blatantly lied even to Angela Merkel when she was Federal Chancellor and now lies to Olaf Scholz and Emmanuel Macron. He was just lying to them on the eve of the invasion of Ukraine. He's not really interested in Western public opinion now, and it's clear that he's not going to be able to use the friends he had there in the West anytime soon, because now there's no one there on a platform of friendship with Putin's Russia to get support any more.*"[45]

[43] П. Соболев, "Путин хочет превратить Россию в самодостаточную осажденную крепость," *Rus.Postimees*, March 18, 2022, https://rus.postimees.ee/7479485/morozov-putin-hochet-prevratit-rossiyu-v-samodostatochnuyu-osazhdennuyu-krepost.

[44] Ibid.

[45] Ibid.

I argue that sometimes Morozov spread other ideas and these ideas should be analyzed very carefully, while there are narratives and ideas that at least covertly justified Russian imperialism, but also Morozov also used some Marxist ideas and theories.

Therefore, we'll take the most important of Morozov's works, his only monograph in English, and look at some of the ideas he developed in it. Some scholars who analyzed this work accused Morozov of spreading several ultra-leftist views in his scientific works.[46]

It was clearly shown by Estonian scholar Dr. Peeter Espak who analyzed some of Morozov's works and showed in his short analysis of Morozov's book *Russia's Postcolonial Identity: A Subaltern Empire in a Eurocentric World* (published in 2015) that this opus is full of radical left ideas and even some pseudo-theories, and an attempt to create a self-sufficient system or political economy of historical philosophy on the basis of all this, the discussion is in fact devoid of any rational systematicity.[47]

Peeter Espak highlight the main arguments of Morozov "*essence of which only some of the reasoning and conclusions should have made the hairs on the head of any thinking person who is not a Russian imperialist and/or Trotskyist revolutionary stand up in anger and all the red fires light up wherever they are.*"[48] For example, Morozov argued: "*I would argue that twentieth-century Marxism and its intellectual heirs such as world-systems theory can provide us with additional conceptual tools, enriching our analysis. As I have repeatedly pointed out, especially in Chapter 2, I see a key strength of postcolonial theory as applied to Russia in its ability to integrate different levels of analysis, and in particular to see domestic developments as conditioned by such global phenomena as colonialism and Eurocentrism.*"[49]

[46] See, e.g., Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

[47] Peeter Espak, "Venemeelne ja läänevastane marksist Vjatšeslav Morozov," *Err*, January 20, 2024, https://www.err.ee/1609228107/peeter-espak-venemeelne-ja-laanevastane-marksist-vjatseslav-morozov.

[48] Ibid.

[49] Viacheslav Morozov, *Russia's Postcolonial Identity: A Subaltern Empire in a Eurocentric World* (Palgrave Macmillan, 2015), 84.

Therefore, there is no doubt that Viacheslav Morozov in his book sympathizes with Marxism, among others highlighting, "i*n a fascinating twist of conceptual history, the external dimension was brought up again in the debate between two Marxist thinkers—Mikhail Pokrovsky, a student of Kliuchevsky, and Leon Trotsky (see Etkind 2011: 86–87).*"[50]

Sanshiro Hosaka who mentioned Morozov's positive attitude to Marxism, highlighted that Morozov "*could work only for the handlers he respects and finds politically and intellectually stimulating. If someone imagines GRU handlers as Spetsnaz guys in military uniforms, they've seen too many B-movies. Intelligence theories say that handlers (agenturisty) have sophisticated civilian covers (scholars, journalists, etc.) and should treat Morozov as a soulmate, listening to him carefully, caring about what he is concerned about, and sometimes giving friendly advice. His unnamed handlers, as mentors, perhaps exercised greater ideological influence on Morozov than philosophers such as Ernesto Laclau and Chantal Mouffe, who Morozov often cites in his publications.*" [51]

Peeter Espak showed in his analysis that Morozov's book presented fanatical ideas and pseudo-theories (old-school Marxism, Trotskyism, modern pseudo-scientific ideas). According to Espak, Morozov's monograph "*is a presentation of emotions and wishful thinking, of personal convictions that are so ambiguous and even contradictory, and at times simply a presentation of utterly irrelevant.*"[52]

As a scholar I agree with Hosaka's and Espak's assessments and arguments about Morozov work, and therefore, a deeper analysis of Morozov's works would be useful and relevant to better understand how GRU agents operate in the scientific and academic environment and what messages and narratives they convey through their works and lectures. In Morozov's book, the reader can not only find many leftist ideas, such

[50] Ibid, 33.

[51] Sanshiro Hosaka, "Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal," *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

[52] Peeter Espak, "Venemeelne ja läänevastane marksist Vjatšeslav Morozov," *Err*, January 20, 2024, https://www.err.ee/1609228107/peeter-espak-venemeelne-ja-laanevastane-marksist-vjatseslav-morozov.

as Trotsky's economic theories and other Marxist ideas, but even also narratives and ideas promoted by Putin's regime. Let us start with Morozov's main arguments that the Russian Federation must be viewed as a subaltern empire.[53]

Morozov also promoted similar ideas in his lectures and popular-scientific texts. In one of these published in 2021, Morozov argues (basically using Russian propaganda narrative of Russophobia), that Russian "*elites consider themselves representatives of Europe in Russia, but at the same time they do not feel themselves full-fledged Europeans in Europe, because in Europe, Russia is still perceived as a peripheral, semi-barbaric state—the mythology with bears, balalaikas, and other things exists in various forms throughout practically the entire New Age.*"[54]

Morozov emphasized Russia's uniqueness: "*It is also important here that Russia lacks a language that would allow it to somehow describe its own uniqueness."[55] He also highlighted the uniqueness of the USSR as an empire.[56] He also called modern Putinism a unique phenomenon: "Putinism is based is probably unique, in structural terms it is a symptom of a much more enduring predicament that Russia has faced throughout its modern history.*"[57]

This idea about the "uniqueness" of Russia and the Russian soul, etc., is already a pro-Kremlin, pro-imperial narrative about Russia's special path[58] (*osobyi put'* in Russian) and uniqueness, for example, Putin called Russia

[53] Viacheslav Morozov, *Russia's Postcolonial Identity: A Subaltern Empire in a Eurocentric World* (Palgrave Macmillan, 2015), 1.

[54] Л. Гарипова, "Вячеслав Морозов. Россия/СССР – особая империя?" *Сигма*, March 14, 2021, https://syg.ma/@leisan-garipova/viachieslav-morozov-rossiia-sliesh-sssr-osobaia-impieriia. See also: В Морозов, "Subaltern Studies. Лекция по курсу «(Пост)колониальные исследования» в рамках проекта «Ташкент-Тбилиси»" (2021).

[55] Ibid.

[56] Гарипова, 2021.

[57] Viacheslav Morozov, *Russia's Postcolonial Identity: A Subaltern Empire in a Eurocentric World* (Palgrave Macmillan, 2015), 154.

[58] This term is often used in Russia with propagandistic purposes. В. Шевченко, "Особый путь развития России: миф или реальность?" Проблемы цивилизационного развития 2 (2022). See also: Igor Kopõtin and Vladimir Sazonov, "The Russian Military's Use of History to Create a Post-Soviet Identity: The Development of Conceptual Understandings from the 1990s to the Mid-2000s," *The Journal of Slavic Military Studies*, 36(4) (2023): 410–434.

a unique country.[59] However, it is quite old and has its roots in the 19th century. When Count Sergey Uvarov (1786–1855) lived and Slavophiles were active, the idea of Russia's uniqueness was taken up afterwards by Eurasianists such as Ivan Ilyin,[60] who lived in exile and other Russian philosophers who spoke about the "Russian idea."[61] Morozov repeats these ideas and even develops them: "*In this sense, Russia is part of the pan-European space, but still a special part. It is connected with management practices, with economic structure, with resource dependence, with identity, with orientation and self-orientation, with the lack of full recognition as a European power. The element of subalternity is manifested on the one hand in identification with Europe, and on the other hand in a structurally conditioned sense of otherness and subordination, even, perhaps, inferiority.*"[62]

At the same time Morozov tries to distance himself, but still his arguments trace Russia's resentment towards Europe and oppression and discrimination against Russia, which fits perfectly into the Kremlin's propaganda narrative of Russophobia,[63] which goes back to the 19th century, to the era following the Crimean War (1853–1856). Morozov writes "*In this sense, Russia is part of the pan-European space, but still a special part. This is due to its governance practices, economic structure, resource dependence, identity, orientation and self-orientation, and lack of full recognition as a European power. The element of subalternity manifests itself, on the one hand, in identification with Europe and, on the other, in a structurally conditioned sense of otherness and subordination, perhaps even inferiority. It is sometimes exacerbated, sometimes attempted to be erased, but it is defined precisely by the fact that Russia feels itself to be part of Europe…*"[64]

[59] "Путин назвал, в чем состоит уникальность России," ИА Красная Весна, November 25, 2024, https://rossaprimavera.ru/news/89263315https://rossaprimavera.ru/news/89263315.

[60] Ivan Ilyin (1883–1954) was a Russian philosopher, fascist, and a White Guard emigre. Ilyin's ideas are said to have strongly influenced the worldview of Putin, who is very fond of reading Ilyin and has been called Putin's philosopher.

[61] Н. Бердяев, *Русская идея. Основные проблемы русской мысли XIX века и начала XX века* (Париж 1946).

[62] Л. Гарипова, "Вячеслав Морозов. Россия/СССР – особая империя?" *Сигма*, March 14, 2021, https://syg.ma/@leisan-garipova/viachieslav-morozov-rossiia-sliesh-sssr-osobaia-impieriia.

[63] See about Russophobia in Morozov's book: Viacheslav Morozov, *Russia's Postcolonial Identity: A Subaltern Empire in a Eurocentric World* (Palgrave Macmillan 2015), 115–120.

[64] Л. Гарипова, "Вячеслав Морозов. Россия/СССР – особая империя?" *Сигма*, March 14, 2021, https://syg.ma/@leisan-garipova/viachieslav-morozov-rossiia-sliesh-sssr-osobaia-impieriia.

Concluding Notes

Analyzing Morozov's activities at the University of Tartu, including scholarly works and his texts as opinion leader, I can conclude the following:

First, one gets the impression that Morozov was not only engaged in information gathering, but also his academic activities were often related with pro-Kremlin discourse and supporting Russian imperialism.

Second, even if the GRU did not interfere in his academic activities (which I doubt), he was spreading extreme Marxist ideas in the academic environment, as Soviet intelligence and the so-called Cambridge five[65] in the 1930s and much later the USSR did during the Cold War, with the aim of reinforcing ideological frictions in the community in order to further polarize Western society.

Third, although Morozov sometimes criticized the Putin regime in his works, he did so with some restraint and almost always tried to defend Russian imperialism and Russia's aggressive foreign policy agenda, calling Russia a "subaltern empire" that has been outdone and spreading the idea that Russia is a unique country, including the Putin regime. Among other things, he raised the issue of Russophobia and other Russian propaganda narratives.

However, the question arises how such a person could have been working at the University of Tartu for almost fourteen years, given the fact that we were warned about Morozov's writings as early as in 2005 by Jeroen Bult[66] and that rumors had been circulating in Tartu for years that there was a professor of political science at the Skytte Institute of the University of Tartu who was a Russian spy.[67]

Morozov's devastating activities are hard to estimate, he published a huge number of scientific articles in influential journals abroad and in Estonia,

[65] Richard Trahair, *Encyclopedia of Cold War Espionage, Spies, and Secret Operations* (Enigma Books, 2012), 489–652.

[66] Jeroen Bult, "Baltimaad – kas "uue" Euroopa esmaasukad?" *Diplomaatia* (October 2005), https://diplomaatia.ee/baltimaad-kas-uue-euroopa-esmaasukad/.

[67] Urmas Sutrop, "Spionaažis süüdistavat Morozovit jälgiti juba kümmekond aastatz," *Postimees*, January 22, 2024, https://arvamus.postimees.ee/7943588/urmas-sutrop-spionaazis-suudistavat-morozovit-jalgiti-juba-kummekond-aastat.

he published reports and analyses on Russian politics, he was an opinion leader and presented his vision in Estonian, Russian, and English, he was popular among students who studied in English at the University of Tartu, he supervised BA, MA, and PhD theses, organized major international conferences, and received awards and grants. In addition to all this, he was also secretly engaged in spying in Estonia for more than thirteen years, having been recruited by the GRU nearly thirty years ago. This is a good example of how academia can be used by the Russian special services to carry out their influence operations.

Policy Recommendations

While the espionage activities of Russian spy Morozov at the University of Tartu are acknowledged, the academic world needs to prepare for such threats and challenges in the future. The interest of Russian and Chinese intelligence services in Western scientists, their research, students, and universities is increasing.

The following steps and measures should be considered to prevent or minimize such threats:

Firstly, in the case of Morozov, there were a number of warning signs that Morozov might be linked to the Russian special services, as there were rumors in academic circles in Tartu for several years that a Russian professor working as a political scientist at the University of Tartu was a spy. These kind of signs should be taken seriously and not ignored by scientists and university management.

Secondly, an article published in Estonian think-tank's newspaper *Diplomaatia* in 2005 (five years before Morozov was hired at the University of Tartu) contained a thoughtful article on Morozov's pro-Russian views and the ideas he promoted in his works.

Thirdly, in several of his works and appearances, Morozov propagated extreme Marxist (e.g., Trotskyist) ideas and at same time defended Putin's Russian policy and promoted the idea of a multi-polar world, which is basically Primakov's doctrine main postulate. One gets the impression that his colleagues did not read his works enough, or that the content of their research was not paid attention to and taken seriously by Morozov's pro-Kremlin activities, which were often hidden, but still identifiable.

On this basis, I would suggest that consideration be given to carrying out background checks on all non-Western academics, including what and where they have studied, worked, and what ideas they disseminate. This is a huge and complex but necessary task to protect the Western academic environment. The West's own scientists are also at risk, as they can be recruited, influenced, and blackmailed by the special services of Russia, China, and Iran, etc., so they too should be checked (at least randomly).

In addition, it is important to raise awareness among Western researchers, students, academic staff, and society in general about the security threats is crucial—especially threats posed by Russia and China, including, in particular, information about information influence activities (e.g., disinformation) and espionage. Increasing critical thinking of people in the Western academic environment should be a priority while they are teaching students, future decision-makers in politics, economics, culture, and society. Western researchers are creating new knowledge and know-how that should be protected from hostile countries and organizations, as well as from hostile impact and espionage.

Universities considering taking on academics (especially from outside NATO, the EU, and the wider world) need to be aware of the danger that a researcher or university lecturer from abroad could turn out to be a spy working for, say, the Chinese or Russian military intelligence. He or she could also potentially be a saboteur, a technology thief, or an agent of influence, for example, with the aim of creating a spy network or causing damage. In this respect, great caution should be exercised, potential researchers and academics who promote some extremist and imperialist ideas (e.g., pro-Kremlin views, etc.) should be very carefully screened and considered for employment. However, it should not be excluded that a seemingly ordinary, calm, and quite moderate-minded top scientist or university teacher may also turn out to be a spy. The challenges are therefore many, and it is difficult to solve them. At the same time, the academic world must remain free, sober-minded, and not indulge in witch-hunts, suspecting potentially everyone, which will only create frustration, spread fear, and may stifle scientific discovery and progress in science.

Bibliography

Aaspõllu, Huko. “Sinisalu: Venemaal tegeleb Eesti-vastase luuretegevusega sadu inimesi.” Err, January 21, 2024, https://www.err.ee/1609227084/sinisalu-venemaal-tegeleb-eesti-vastase-luuretegevusega-sadu-inimesi.

Бердяев, Николай. *Русская идея. Основные проблемы русской мысли XIX века и начала XX века* (Париж, 1946).

Bult, Jeroen. “Baltimaad – kas “uue” Euroopa esmaasukad?” *Diplomaatia* 25, October 2005, https://diplomaatia.ee/baltimaad-kas-uue-euroopa-esmaasukad/.

Einmann, Andres. “GRU värbas Eestis luuranud professori juba 1990. aastate alguses.” *Postimees*, June 19, 2024, https://www.postimees.ee/8043515/gru-varbas-eestis-luuranud-professori-juba-1990-aastate-alguses.

Espak, Peeter. “Venemeelne ja läänevastane marksist Vjatšeslav Morozov.” Err, January 20, 2024, https://www.err.ee/1609228107/peeter-espak-venemeelne-ja-laanevastane-marksist-vjatseslav-morozov.

Estonian Internal Security Service Annual Review 2023–2024, Estonian Internal Security Service 2024, accessed July 21, 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf

Estonian Internal Security Service Annual Review 2024–2025, accessed December 29, 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf

Hosaka, Sanshiro. “Jaapani politoloog Sanshiro Hosaka: minu arvamus Morozovi kohtuotsuse taustal.” *Vabariik*, June 30, 2024, https://vabariik.ee/kolumn/jaapani-politoloog-sanshiro-hosaka-minu-arvamus-morozovi-kohtuotsuse-taustal/.

Гарипова, Лейсан. “Вячеслав Морозов. Россия/СССР – особая империя?” *Сигма*, March 14, 2021, https://syg.ma/@leisan-garipova/viachieslav-morozov-rossiia-sliesh-sssr-osobaia-impieriia.

Катенова, Юлия. “Песков: Россия не угрожает никому в Европе,” *Парламентская газете*, April 26, 2024, https://www.pnp.ru/politics/peskov-rossiya-ne-predstavlyaet-ugrozy-ni-dlya-kogo-v-evrope.html.

Koort, Erkki. “Venemaa sõjaväeluure spioon Tartus ja Eesti sihtmärgid Venemaal.” *Postimees*, June 21, 2024, https://arvamus.postimees.ee/8045133/erkki-koort-venemaa-sojavaeluure-spioon-tartus-ja-eesti-sihtmargid-venemaal

“Kohus mõistis Viatcheslav Morozov süüdi luuretegevuses,” *Kaitsepolitseiamet*, June 18, 2024, https://kapo.ee/et/content/kohus-moistis-viatcheslav-morozov-suudi-luuretegevuses/.

Kopõtin, Igor and Vladimir Sazonov. “The Russian Military’s Use of History to Create a Post-Soviet Identity: The Development of Conceptual Understandings from the 1990s to the Mid-2000s.” *The Journal of Slavic Military Studies*, 36 no. 4 (2023): 410–434.

Kuckartz, Udo. *Qualitative Text Analysis: A Guide to Methods. Practice & Using Softwar*e. Sage Publications, 2014.

Ломп, Лоора-Элизабет. “Студенты: задержанный по подозрению в шпионаже против Эстонии преподаватель относился к России скорее критически.” *Rus.Postimees*, 16 January, 2024, https://rus.postimees.ee/7939521/studenty-zaderzhannyy-po-podozreniyu-v-shpionazhe-protiv-estonii-prepodavatel-otnosilsya-k-rossii-skoree-kriticheski.

Morozov, Viacheslav. “Russia and the West: playing by the rules? \ Venemaa ja Lääs: mäng reeglite järgi?” *Diplomaatia* 74/75, November 2009, https://diplomaatia.ee/venemaa-ja-laas-mang-reeglite-jargi/.

Morozov, Viacheslav. “Ceurus meelitab Tartusse tunnustatud teadlasiz.” *Universtas Tartuensis* 5, May 2013, https://www.ajakiri.ut.ee/artikkel/947.

Morozov, Viacheslav. *Russia’s Postcolonial Identity: A Subaltern Empire in a Eurocentric World*. Palgrave Macmillan, 2015.

Morozov, Viacheslav et al. “Vene rehepapp, Kremli välispoliitika populaarsus ja de facto riigid.” *Riigikogu Toimetised* 40 (2019): 75–85.

Морозов, Вячеслав. “Subaltern Studies. Лекция по курсу «(Пост)колониальные исследования» в рамках проекта «Ташкент-Тбилиси»” (2021).

Морозов, Вячеслав. “Война с Украиной положила конец истории постсоветской России.” *Rus.Err*, March 4, 2022, https://rus.err.ee/1608520970/vjacheslav-morozov-vojna-s-ukrainoj-polozhila-konec-istorii-postsovetskoj-rossii.

Paris, Krister. “Vjatšeslav Morozov: ebakinda ja haavatavana tunneb end mitte niivõrd lääs kui hoopis Venemaa.” *Eesti Päevahaleht*, March 29, 2021, https://

epl.delfi.ee/artikkel/92983781/intervjuu-vjatseslav-morozov-ebakinda-ja-haavatavana-tunneb-end-mitte-niivord-laas-kui-hoopis-venemaa.

“Путин назвал, в чем состоит уникальность России.” *ИА Красная Весна*, November 25. 2024, https://rossaprimavera.ru/news/89263315https://rossaprimavera.ru/news/89263315.

“Путин заявил о ставшем реальностью многополярном мире.” *РБК*, July 4, 2024, https://www.rbc.ru/rbcfreenews/66865a079a794793ab095cb3.

Radin, Andrew. *Hybrid Warfare in the Baltics: Threats and Potential Response*s. Rand Corporation, 2017.

“«Россия не представляет угрозы для Запада»: SIPRI подсчитал военные расходы стран.” *Военное обозрение*, June 1, 2024, https://topwar.ru/243580-rossija-ne-predstavljaet-ugrozy-dlja-zapada-sipri-podschital-voennye-rashody-stran.html.

Sazonov, Vladimir, Erkki Koort, Priit Heinsoo and Kadri Paas. *Introduction of Hybrid Threats of Internal Security*. Estonian Academy of Security Sciences, 2020.

Шевченко, Владимир. “Особый путь развития России: миф или реальность?” *Проблемы цивилизационного развития* 2 (2022): 43–69.

Соболев, Павел. “Путин хочет превратить Россию в самодостаточную осажденную крепость.” *Rus.Postimees*, March 18. 2022, https://rus.postimees.ee/7479485/morozov-putin-hochet-prevratit-rossiyu-v-samodostatochnuyu-osazhdennuyu-krepost.

Sutrop, Urmas. “Spionaažis süüdistavat Morozovit jälgiti juba kümmekond aastat.” *Postimees*, January 22, 2024. https://arvamus.postimees.ee/7943588/urmas-sutrop-spionaazis-suudistavat-morozovit-jalgiti-juba-kummekond-aastat.

Trahair, Richard. *Encyclopedia of Cold War Espionage, Spies, and Secret Operations*. Enigma Books, 2012, 489–652.

“Venelaste jaoks luuranud Tartu Ülikooli professor Vjatšeslav Morozov saadeti kuueks aastaks vangi.” *Reporter.ee*, June 18, 2024, https://reporter.kanal2.ee/8043436/venelaste-jaoks-luuranud-tartu-ulikooli-professor-vjatseslav-morozov-saadeti-kuueks-aastaks-vangi.

https://doi org/10 59862/k7m2x9q4r8/12

Chapter 12

Situating Academia in Economic Security Strategies: Lessons from Taiwan

MARCIN MATEUSZ JERZEWSKI
ORCID 0009-0004-9187-2636
European Values Center for Security Policy (Taipei, Taiwan)

Abstract: The text analyzes Chinese coercive strategies targeting the cognitive domain, both in terms of academia and key technological sectors, identifying critical gaps in those domains in reference to the Copenhagen school of IR. Apart from identifying threats connected to the erosion of academic freedom (limiting research and innovation potential, but also free and open academic environment), as well as critical technologies, having strategic importance for the security of Taiwan, the report provides also political advisory to other countries, including integration of research security into national security strategies, implementation of tiered international cooperation system, restriction of access to sensitive research facilities, as well as establishment of capacity-building initiatives fund.[1]

Keywords: Taiwan, academia, economic security, research security, talents, technology

A part of the Huntingtonian third wave,[2] Taiwan is a democratic success story. Its transition from the authoritarianism of the White Terror era (1949–1992) to the robust and inclusive democracy it is today also created an environment conducive to fostering the production of knowledge and unobstructed discourse in the academic sphere. Its dedication to civil liberties is reflected in its

[1] The keywords and abstract of this report is based on the text provided by the Author, but was generated by the Editors.

[2] Samuel Huntington, "Democracy's Third Wave," Journal of Democracy 2, no. 2 (1991): 12–34.

high scores in Freedom House's annual Freedom in the World report[3] and its ranking of 37th globally—and first in Asia—in the 2023 Academic Freedom Index, a comprehensive global assessment of academic freedom.[4] These achievements underscore the "democracy-education nexus," which frames procedural democracy and academic freedom as mutually reinforcing processes.[5]

However, Taiwan's hard-won democratic system, including academic freedom, faces significant threats due to increasing geopolitical volatility. The Beijing regime claims Taiwan, Penghu, Kinmen, and Matsu as part of its own territory despite never having controlled them and has not renounced the use of force to annex them. While China's coercive tactics are evident in traditional domains of warfare (land, air, sea, space, and cyberspace),[6] its influence increasingly extends into the emerging sixth domain, the cognitive domain,[7] targeting academia. This aligns with broader efforts by the Chinese Communist Party to manipulate culture, education, and media to influence democracies.[8]

Chinese influence in Taiwanese academia operates mainly on two key pillars: people and technology. The first pillar involves shaping narratives about China and cross-strait relations,[9] promoting self-censorship,[10] and leveraging academic exchanges to apply economic pressure on Taiwanese universities reliant on full-fee-paying Chinese students amid domestic demo-

[3] "Taiwan," Freedom in the World, Freedom House, https://freedomhouse.org/country/taiwan.

[4] "Academic Freedom Index," Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), and the V-Dem Institute, 2024. https://academic-freedom-index.net/.

[5] John Dewey, Democracy and Education (Simon and Schuster, 1997); Jantha Sisira Kumara and Ramanie Samaratunge, "The Effect of Academic Freedom on Electoral Democracy in the Asian Region," Public Administration and Development 44, no. 3 (2024): 137–149.

[6] James A. Siebens, China's Use of Armed Coercion (Taylor & Francis, 2023); Bonny Lin et al., "A New Framework for Understanding and Countering China's Gray Zone Tactics," RAND Corporation (blog), March 30, 2022, https://www.rand.org/pubs/research_briefs/RBA594-1.html.

[7] Ying-Yu Lin, "China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures," Taiwan Strategists, no. 20 (2023): 37–54

[8] Doublethink Lab, "CITW 2023 in Taipei: Uniting to Counter Evolving PRC Threats," Medium, July 10, 2024, https://medium.com/doublethinklab/citw-2023-in-taipei-uniting-to-counter-evolving-prc-threats-e5ea4fdbecb8.

[9] Yu-Li Wang and Luc Chia-Shin Lin, "Is Involvement Effective? A Case Study of Exchange Programs' Influence on Mainland Chinese Communications Major Exchange Students' Support for Taiwan," Journal of Cross-Strait Relations 27, no. 2 (2023): 316–335.

[10] Jaw-Nian Huang, "China's Influence on Taiwan's Media: A Model of Transnational Diffusion of Chinese Censorship," in China's Influence and the Center-Periphery Tug of War in Hong Kong, Taiwan and Indo-Pacific, ed. Brian C. H. Fong, Jieh-min Wu and Andrew J. Nathan (Routledge, 2020), 205–223, https://doi.org/10.4324/9781003088431-17.

graphic challenges.[11] The second pillar highlights the strategic link between economic and academic security. China seeks to dominate key technological sectors, such as semiconductors and dual-use technologies, to advance its hegemonic ambitions.[12]

Taiwan's approach to knowledge security must address these threats, recognizing the critical intersection of academic freedom, national security, and economic resilience as it faces increasing belligerence from its authoritarian neighbor. The objective of this paper is thus twofold. Firstly, it provides a comprehensive overview of Taiwan's economic security and academic security policies, identifying critical overlaps and gaps. Secondly, it evaluates the current framework in light of the geopolitical situation around Taiwan and draws positive and negative lessons for other democracies seeking to build up their academic security agendas.

The Copenhagen School Comes to Taipei: The Emergence of Economic Security and Research Security

The inclusion of concerns related to economic and academic affairs in security discourse reflects the debate between "traditionalists" and "wideners" in the field of security studies. The first group of scholars, largely affiliated with the realist school, tends to restrict the subject to politico-military issues. Meanwhile, the wideners, whose views generally stem from constructivist theories of international relations, seek a more holistic approach to security, which includes the economic, societal, and environmental sectors.

Within the broad "wideners" camp, the Copenhagen School's concept of securitization, in particular, provides a robust framework for analyzing academia and research security as critical areas of inquiry in security studies. Securitization, as Wæver describes, is a "speech act" that involves framing

[11] Ralph Jennings, "For Mainland Chinese Students, Taiwan's Universities Are 'like Paradise.' But there's a catch," Los Angeles Times, March 26, 2017, https://www.latimes.com/world/asia/la-fg-taiwan-china-students-2017-story.html.

[12] Tzu-I Lee, "Bordering Secrecy: An Empirical Study on Cross-Border Trade Secret Misappropriation in the Semiconductor Sector," Connecticut Journal of International Law 39, no. 2 (2024): 166–237, https://ssrn.com/abstract=4827530; Larry Diamond, James O. Ellis and Orville Schell, eds., Silicon Triangle: The United States, Taiwan, China, and Global Semiconductor Security (Hoover Institution Press, 2023).

an issue as an existential threat through discourse, irrespective of the threat's objective reality, and legitimizing extraordinary measures to address it.[13]

This discursive process entails four key components: securitizing agents, threats, referent objects, and the audience. In the case of securitization of academic research, governments of liberal democracies act as securitizing agents, framing the involvement of malign authoritarian actors with their research institutions as threatening to their normative and tangible interests. These threats include the erosion of academic freedom and the irregular transfer of strategic technologies. The referent object in this process is a free and open academic environment with robust research and innovation capacity that supports the development of strategic, high-tech outputs. Last but not least, the audience includes academic elites and private sector executives reliant on academia-industry cooperation to materialize such outputs.

By framing the protection of the integrity of research institutions and processes as vital to national security, liberal democracies, including Taiwan, construct a foundation for the adoption of research security measures. This demonstrates how securitization theory enables us to understand the interplay between academic security, economic security, and geopolitical volatility in the evolving landscape of global security.

Towards the Emergence of Intertwined Economic Security and Research Security Regimes

In the Taiwanese context, the discursive process of securitization is inherently tied to the country's complex relationship with the People's Republic of China. On the one hand, as the People's Republic of China defines the "resolution of the Taiwan issue"—implying annexation of its territory—as a core objective within its strategy of "Great Rejuvenation of the Chinese Nation" (中華民族偉大復興), Taiwan faces an existential threat amid a sustained coercive campaign carried out across various domains.

On the other hand, economic links between Taiwan and China remain strong. Amid the "Taiwan Miracle" of the mid-1980s, Taiwanese businesspe-

[13] Ole Wæver, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (Columbia University Press, 1995), 46–86.

ople (台商, taishang) began to play an influential role in linking China with global markets by exporting capital, managerial know-how, and capitalist ideology of efficiency across the Taiwan Strait.[14] The growth in the frequency and volume of cross-strait exchanges in economic and social realms created economic dependencies between both sides. This phenomenon also became consequential for research security, given the intensification of academic exchanges between both sides and the appetite to capitalize on China's burgeoning market's hunger for cutting-edge technologies.

The expanding dependencies on China generated externalities for Taiwan's domestic politics. Citizens grew increasingly concerned that continued expansion of economic relations with China would erode Taiwan's autonomy and increase Beijing's influence over its democratic processes and institutions. This led to the inception of the 2014 Sunflower Movement.[15] One of the triggers of this bottom-up mobilization was the proposed Cross -Strait Service Trade Agreement, which the then-ruling Chinese Nationalist Party (Kuomintang) sought to pass without a clause-by-clause review in the Legislative Yuan. The movement contributed to the landslide victory of the pro-sovereignty Democratic Progressive Party in 2016,[16] which implemented measures to manage risks associated with excessive economic dependence on China. Although these policy responses were implemented before the advent of the term "de-risking," they effectively function as de-risking strategies which underpin Taiwan's approach to economic security.[17]

In the Taiwanese context, the existing research security measures focus primarily on the protection of critical technologies that have strategic importance for national security. Previous studies on research security in Taiwan pointed to the limited understanding of this concept as a distinct policy concern or subject

[14] Shelley Rigger, *The Tiger Leading the Dragon: How Taiwan Propelled China's Economic Rise* (Stanford University Press, 2020).

[15] Ming-sho Ho, *Challenging Beijing's Mandate of Heaven: Taiwan's Sunflower Movement and Hong Kong's Umbrella Movement* (Temple University Press, 2019).

[16] Ming-sho Ho and Thung-hong Lin, "The Power of Sunflower: The Origin and the Impact of Taiwan's Protest against Free Trade with China," in *The Umbrella Movement*, ed. Ming-sho Ho and Thung-hong Lin (Amsterdam University Press, 2017).

[17] Jakub Janda et al., "Fortifying Economic Security: The EU's Response to China's Risk," Wilfried Martens Centre for European Studies, June 17, 2024, https://www.martenscentre.eu/publication/fortifying-economic-security-the-eus-response-to-chinas-risk/.

of academic inquiry.[18] Many economic security and research security issues are governed by the same laws and overseen by the same executive agencies.

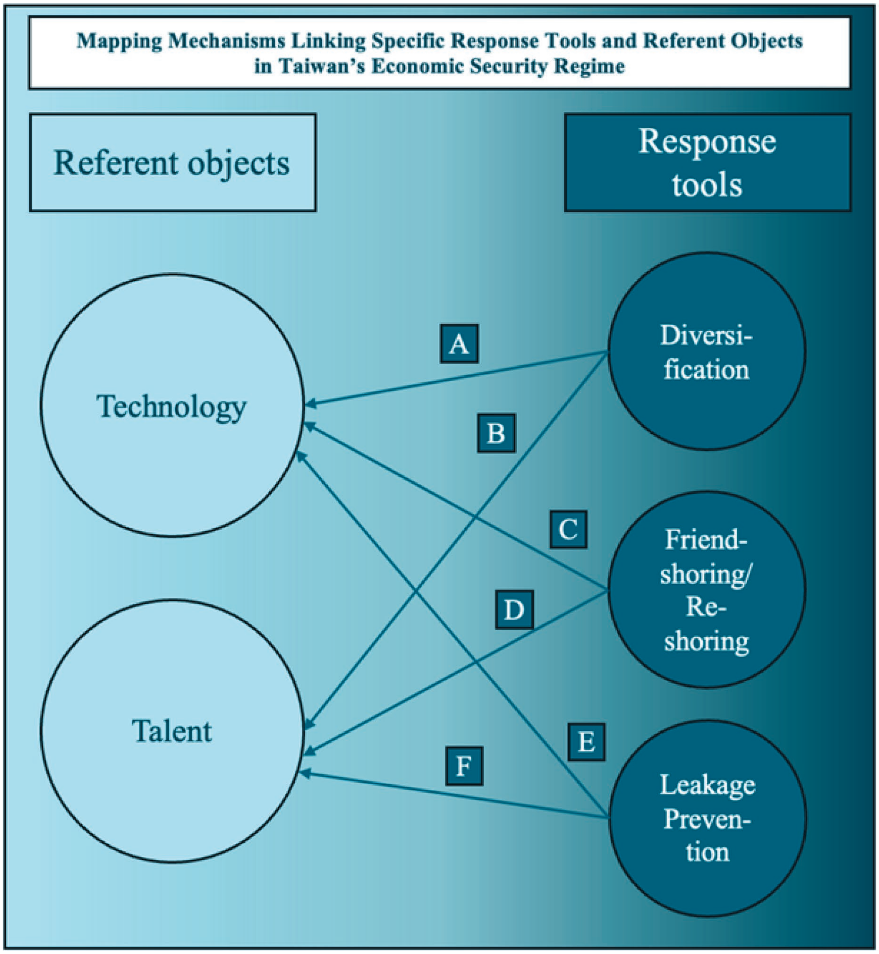
Mapping Mechanisms Linking Specific Response Tools and Referent Objects in Taiwan's Economic Security Regime
Referent objects
Response tools
Technology
Talent
Diversi-fication
Friend-shoring/ Re-shoring
Leakage Preven-tion
A
B
C
D
E
F

Figure 1. Mapping Mechanisms Linking Specific Response Tools and Referent Objects in Taiwan's Economic Security Regime

Source: Author's own elaboration.

For legend, see Appendix 1.

[18] Ingrid d'Hooghe and Jonas Lammertink, "How National Governments and Research Institutions Safequard Knowledge Development in Science and Technology," *Leiden Asia Center*, November 2022, https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safequard-Knowledge-Development-in-Science-and-Technology.pdf.

As illustrated in Figure 1, the Taiwanese economic security regime can be parsimoniously operationalized as consisting of two referent objects: (1.1) technology protection and (1.2) talent control, and three response tools: (2.1) diversification of economic relations, (2.2) friendshoring and reshoring, and (2.3) limiting the leakage of strategic technologies. Among the three tools enumerated here, the third one is most relevant to understanding the focus of Taiwan's research security regime. Therefore, the following sub-section provides a brief overview of the first two tools for context, while the subsequent sub-section offers a more in-depth perspective on the evolution of strategic technologies protection regime with implications for both economic security and research security.

Diversification, Friendshoring, and Reshoring as Tools of Economic Security

Taiwan's diversification strategy is central to its de-risking efforts. The key strategy underpinning this endeavor is the New Southbound Policy (新南向政策; NSP). Launched under President Tsai Ing-wen, the NSP targets eighteen countries in South and Southeast Asia and Oceania and is centered around four pillars: economic and trade cooperation, people-to-people exchanges, resource sharing, and regional connectivity.[19] By promoting investment and production relocation, the policy has strengthened Taiwan's presence in the emerging markets of its neighborhood.[20] In terms of reducing economic dependencies on China, the policy bore fruit, as in 2022 Taiwan's investments in South and Southeast Asia reached €4.8 billion in 2022, surpassing–for the first time–the €4.62 billion invested in China. This trend intensified in 2023, with investments in the region totaling €3.97 billion, compared to €1.16 billion in China.[21]

[19] Alan Hao Yang, "Strategising Taiwan's New Southbound Policy by the Practice of PPPP Configuration," *Journal of Contemporary East Asia Studies* 10, no. 1 (2023): 45–62.

[20] Shih-chung Liu, "The Impact of U.S.-China Trade Friction on Both Countries and the Global Economy," Prospects & Perspectives, no. 8 (2018): 1–4, https://www.pf.org.tw/tw/pfch/33-7901.html.

[21] "王美花：南亞東南亞投資額首超中國　新南向里程碑 (Wang Mei-Hua: Investment in South and Southeast Asia Surpasses China for the First Time: A Milestone for the New Southbound Policy)," *Central News Agency*, November 29, 2023, https://www.cna.com.tw/news/aipl/202311290399.aspx.

Complementing the NSP, which facilitates friendshoring,[22] the "Action Plan for Welcoming Overseas Taiwanese Businesses" encourages reshoring through incentives such as land, talent, and low-interest financing. The plan, now in its third phase, has attracted 305 enterprises and over TWD 1.2 trillion (approximately €35 billion) in investment, bolstering Taiwan's economic resilience and aligning with net-zero goals.

Prevention of National Core Key Technologies Leakage at the Nexus of Economic Security and Research Security

In addition to diversifying its investment relations, as well as promoting friendshoring and reshoring policies, Taiwan's de-risking strategy incorporates measures to safeguard national core key technologies (NCKT) from exposure to foreign adversaries. These measures can be divided into two categories: technology protection, governed by the National Security Act (NSA), and talent control, which the Act Governing Relations between the People of the Taiwan Area and the Mainland Area (AGRPTAMA) regulates.

The second Tsai Ing-wen administration (2020–2024) sought to recalibrate the focus of the country's security policymaking to new areas of concern, which notably included the issue of strategic technologies leakage. This adjustment was rooted in a growing awareness that Taiwan's leadership in critical technologies, particularly in semiconductors, is a double-edged sword: it bolsters Taiwan's deterrence against potential aggression from China while also making it a target for Chinese technology espionage. Taiwan's advanced semiconductor industry, including critical technologies such as the 14-nanometer process and heterogeneous integration through system-in-package, is crucial not only to global supply chains but also to Taiwan's domestic economy and long-term industrial competitiveness. Protecting these technologies thus became an important focus of lawmakers.

In response to these realities, Taiwan enacted significant legislative changes. In June 2022, the Legislative Yuan passed amendments to the NSA,

[22] Zoë Weaver-Lee, "Taiwan's Companies Look beyond China, But Key Challenges Remain," *Global Taiwan Brief* 8, no. 18 (2023): 12–14, https://globaltaiwan.org/wp-content/uploads/2023/09/GTB-8.18-PDF-Final.pdf.

establishing strict penalties for the leakage of critical technologies. These amendments criminalize economic espionage and prohibit the transfer of technologies critical to Taiwan's national security, economic development, or industrial competitiveness to foreign adversaries. Individuals who breach the revised provisions of the NSA can be subject to imprisonment and fines, including up to twelve years in prison and penalties of up to NT$100 million (approximately €3 million).[23]

To make the enforcement actionable, the Executive Yuan released the first official list of NCKT on December 5, 2023, covering twenty-two items across sectors including defense, space, semiconductors, agriculture, and information security. This list can be reviewed in Table 2 in Appendix 1. As of November 2024, the National Science and Technology Council is also planning to release a "second wave" of NCKT, increasing the total number to thirty-four items.[24] (See Table 3 in Appendix 1). These developments marked a shift from the previous regime, where research and economic security measures were primarily guidelines with limited enforceability. The only known document on research security was the Government-funded National Core Science and Technology Research Program Safety Control Operation Manual. While it provided a comprehensive overview of National Core Technologies (NB: a different term that NCKT introduced by the amendments to the NSA)[25] and delineated related procedures for implementing government-supported projects pertaining to these technologies, it was an administrative guidance rather than a legally binding document. By codifying safeguards for clearly defined NCKTs into law, Taiwan has significantly strengthened its research security regime to counter technological espionage and protect its strategic industries.

[23] Brian Hsiang-Yang Hsieh and Henry Jin-Han Hsieh, "Amended National Security Act Imposes Stricter Punishments on Trade Secret Misappropriation Following New List of Crucial Tech," *IAM Media*, January 17, 2024, https://www.iam-media.com/article/amended-national-security-act-imposes-stricter-punishments-trade-secret-misappropriation-following-new-list-of-crucial-tech.

[24] "國家核心關鍵技術項目及其技術主管機關修正草案 (National Key Critical Technologies and Their Governing Authorities—Revised Draft)," *ROC (Taiwan) National Science and Technology Council*, November 1, 2024.

[25] For details on the National Core Technologies, see Table 1 in Appendix 1.

Relevant changes were also introduced to the AGRPTAMA, which effectively strengthened Taiwan's talent control measures. AGRPTAMA oversees engagements involving individuals from the People's Republic of China, including its Special Administrative Regions of Hong Kong and Macau, in Taiwanese research and tertiary education institutions. While individuals from China who obtain household registration in Taiwan are permitted as faculty members or researchers, they are prohibited from participating in work related to national security or confidential scientific and technological research unless they have maintained household registration in Taiwan for over twenty years.[26]

The recent amendments set forth a review mechanism for cross-strait travel by personnel engaged in NCKT projects commissioned by the government or supported by a government grant. The Mainland Affairs Council explain that there are two categories of individuals who are covered by the new regulations: (1) "individuals or personnel affiliated with legal persons, organizations, or other institutions who are involved in national core technology business that are commissioned by, receive grant from, or are funded by government agencies (institutions) of a certain level;" and "2. those who are involved in the said business or had resigned from their jobs in the said business whose commission, grant, or funding had completed or ended less than 3 years ago."[27]

This is in response to the process of securitization of critical technologies—including tangible assets such as the technologies themselves as well as intangible ones, such as talent—by Taiwan's government agencies. The MAC and the Ministry of Justice Investigation Bureau views talent poaching from Taiwan's semiconductor and high-tech industries as a major risk to the country's global competitiveness and national security.[28] Notably, the MAC explicitly linked the amendments to the NSA, which operationalized technology as a referent object

[26] Mei-chu Huang and Fion Khan, "Thirty locations raided in talent, tech poaching investigations," *Taipei Times*, September 3, 2024, https://www.taipeitimes.com/News/taiwan/archives/2024/09/03/2003823210.

[27] "Executive Yuan Approves the "Draft Amendments to Part of the Provisions of the Act Governing Relations between the People of the Taiwan Area and the Mainland Area," *ROC (Taiwan) Mainland Affairs Council*, February 17, 2022, https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=6A543758F2225F94.

[28] Yu-fu Chen and William Hetherington, "Security act amendments need to be enacted: TSP," *Taipei Times*, August 17, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/08/17/2003804868.

in the process of securitization, and the AGRPTAMA, which operationalizes talent as another referent project. Consequently, the changes to these two core documents ought to be analyzed in tandem when assessing the emergence of intertwined economic security and research security regimes.[29]

Taking Stock: Lessons from Taiwan's Experience in Economic and Research Security

Three main lessons can be enumerated based on the evaluation of Taiwan's experience with attempting an intertwined economic security and research security regime:

1. Embedding Research Security in the National Security Framework While Taiwan does not explicitly define the concept of research security, it clearly integrates relevant mechanisms into its wider security policy framework, including economic security. By addressing vulnerabilities in tangible assets, such as technologies, and intangible ones, such as talent, Taiwan employs a dual approach of incentives and penalties. Measures such as diversification, friendshoring, and reshoring complement the enforcement of strict penalties for technology leakage. However, Taiwan could strengthen the cooperative dimension of research security by fostering collaboration with like-minded partners, particularly under initiatives such as the New Southbound Policy.
2. Context-Specificity of the Taiwan Model Taiwan's research security framework is uniquely tailored to its geopolitical challenges, specifically its adversarial relationship with China. This targeted approach benefits from Taiwan's ability to enact policies that directly address the China threat, leveraging the fact that its relations with the People's Republic of China are generally not considered as state-to-state relations. However, replicating this model in other contexts, such as Central and Eastern Europe states targeting Russia's malign influence in the research domain, may result in significant challenges as democratic coun-

[29] ROC (Taiwan) Mainland Affairs Council. Executive Yuan Approves the "Draft Amendments to Part of the Provisions of the Act Governing Relations between the People of the Taiwan Area and the Mainland Area." February 17, 2022, https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=6A543758F2225F94.

tries need to appropriately balance security measures with cross-border collaboration among trusted partners.

3. Unlocking the Potential of Bottom-Up Initiatives Legislative changes in Taiwan, particularly the amendments to the NSA, made the process of identifying national core key technologies more democratic by involving academics and researchers. The platforming of voices from universities and research institutes addresses a critical need for an inter-sectoral, multi-stakeholder approach to research security. At the same time, further encouragement and financial support for bottom-up initiatives could enhance the acceptance of top-down policies. These initiatives would promote broader stakeholder engagement in safeguarding research security.

Appendix 1: Tables

Area	**Technologies**
Agricultural Science and Technology	Seedling propagation. Cultivation of edible and medicinal mushrooms. Technologies for breeding new crop varieties. Functional genomics and related biochips. Livestock stem cell technology.
Key Manufacturing Technology	Ninety-seven technologies defined in a separate list compiled by the Ministry of Economic Affairs, including seven main sectors: **Semiconductor Technology:** Advanced integrated circuits, wafers exceeding twelve inches in diameter, and related production processes. **Military and Aerospace Equipment:** Aircraft, helicopters, drones, and military-grade components such as engines, rotors, and landing gears. **Advanced Materials and Chemicals:** Fluorinated hydrocarbons, phosphorus compounds, and certain chlorinated chemicals used in specialized applications. **Biotechnology:** Genetic materials, stem cells, and advanced biomedical tools.

Area	Technologies
Key Manufacturing Technology	**Energy and Nuclear Technology:** Nuclear reactors, isotope separators, and associated parts. **Optoelectronics:** Liquid crystal display panels and other high-generation TFT-LCD products. **Pharmaceuticals:** Narcotic drugs, precursors like ephedrine, and medical compounds such as ergot alkaloids and opiates.
Aerospace and Satellite Technology	Aerospace Technology. Remote Sensing Technology and Data. Satellite-Related Technology.
Ocean Science and Technology	Underwater research. Marine geology. Marine physics.
Advanced Integrated Circuit Design and Process Technology	Integrated circuit (IC) manufacturing process at or below three nanometers. IC design at or below five nanometers. Extreme ultraviolet (EUV) lithography technology.
Key Network Security Technology	Key cybersecurity technologies for in-depth defense within the national cybersecurity joint defense system. Core cybersecurity technologies developed to support national missions.

Table 1. National Core Technologies (國家核心科技) defined in the non-legally binding Government-funded National Core Science and Technology Research Program Safety Control Operation Manual (2019, last edited January 2023).

Source: Author's own elaboration based on ROC (Taiwan) National Science and Technology Council, *Government-funded National Core Science and Technology Research Program Safety Control Operation Manual, 5–6.*

Area	Technologies
National Defense Technology	Military Carbon Fiber Composite Materials Technology. Military Carbon/Carbon High-Temperature Ablation-Resistant Materials Technology. Military New Anti-Jamming Identification Friend or Foe (IFF) Technology. Military Microwave/Infrared/Multi-Mode Seeker Technology. Military Active Phased Array Detection Technology. Ramjet Engine Technology.
Space Technology	Satellite Control Technology. Space-Grade X-Band Image Download Technology. Space-Grade Image Compression Electronic Unit (EU) Technology. Space-Grade CMOS Image Sensor Technology. Design, Manufacturing, and Integration of Space-Grade Optical Payload Systems. Space-Grade Active Phased Array Antenna Technology. Space-Grade Passive Reflector Antenna Technology. Space-Grade Radar Image Processing Technology.
Agricultural Technology	Breeding and Propagation Technology—Liquid Strain Cultivation and Monosex Aquaculture Technology. Biochip Technology—Residue Testing for Agricultural Drugs and Biochip Detection of Plant and Animal Pathogens. Agricultural Facility Expert System Technology—Design, Operation, and Maintenance of Greenhouses and Aquaculture Water Environments.
Semiconductor Technology	IC Manufacturing Technology for Processes Below Fourteen Nanometers and Related Key Gases, Chemicals, and Equipment. Heterogeneous Integration Packaging Technology—Wafer-Level Packaging, Silicon Photonics Integration Packaging, and Related Materials and Equipment.
Cybersecurity	Chip Security Technology. Post-Quantum Cryptographic Protection Technology. Network Active Defense Technology.

Table 2. National Core Key Technologies (國家核心關鍵技術) set forth according to Article 3 of the National Security Act.

Source: Author’s own elaboration based on ROC (Taiwan) National Science and Technology Council, *National Key Critical Technologies and Their Governing Authorities—Revised Draft*.

Area	Technologies
Space Technology	Propulsion System Design and Manufacturing for Launch Vehicles Delivering Small Satellites into Orbit. Flight Attitude Determination and Control Technology for Launch Vehicles Delivering Small Satellites into Orbit. Quantum Bit Design and Manufacturing Technology.
Semiconductor Technology	Millimeter-Wave Gallium Nitride (GaN) Power Amplifier Monolithic Microwave Integrated Circuit Design Technology. Gallium Nitride (GaN) Semiconductor Manufacturing Technology for High-Frequency Power Amplifiers. Silicon Carbide (SiC) Semiconductor Manufacturing Technology for High-Voltage Power Components. High-Performance Chip Design Technology for Artificial Intelligence Computing. High-Frequency Wide-Bandwidth High-Density Interconnect Chip Circuit Design Technology. Secondary Battery Cell Technology—High Energy Density and Long Cycle Life Design, Chemical Synthesis, and Manufacturing.

Table 3. Prospective new National Core Key Technologies (國家核心關鍵技術) intended to be added to the list according to Article 3 of the National Security Act and the National Science and Technology Council Regulations for the Identification of National Core Key Technologies.

Source: Author's own elaboration based on ROC (Taiwan) National Science and Technology Council, *National Key Critical Technologies and Their Governing Authorities—Revised Draft.*

Mechanism	Referent Object	Response Tool	Description
A	Technology	Diversification	Promotion of engagements with new target areas, notably through the New Southbound Policy, particularly its "Economic and Trade Cooperation" and "Sharing Resources" pillars.

Mechanism	Referent Object	Response Tool	Description
B	Talent	Diversification	Promotion of engagements with new target areas, notably through the New Southbound Policy, particularly its “People-to-People Exchanges” and “Regional Connectivity” pillars.
C	Technology	Friendshoring/ Reshoring	Allocation of tangible relocation assets through schemes such as Action Plan for Welcoming Overseas Taiwanese Businesses.
D	Talent	Friendshoring/ Reshoring	Efforts deterring sensitive people-to-people engagements, notably including the Mainland Affairs Council’s Eight Must-Knows for Studying in Mainland China.
E	Technology	Leakage Prevention	New punitive mechanisms introduced by the 2022 amendments to the National Security Act.
F	Talent	Leakage Prevention	New review mechanisms introduced by the 2022 amendments to the Act Governing Relations between the People of the Taiwan Area and the Mainland Area.

Table 4. Legend to Figure 1.

Policy Recommendations

Applying Lessons from Taiwan Across Contexts

The lessons from the experience of Taiwan in constructing a research security regime also translate into actionable policy ideas for stakeholders in various contexts. Building upon the lessons learned, the following policy recommendations aim to guide stakeholders in developing robust research security frameworks:

1. Integrate Research Security into National Security Strategies: Recognize research security as a fundamental component of national se-

curity. Engage representatives from the research community in cross-sectoral security policy discussions to ensure comprehensive and informed decision-making.

2. Implement a Tiered System for International Collaboration: Develop a stratified framework that classifies countries based on assessed security risks. This system would regulate access to cross-border research collaborations, balancing the need for academic freedom with necessary security measures. In Taiwan, legislation is clearly pointed toward the People's Republic of China, as the former views the latter as the main origin of security threats. Such narrow targeting might not be feasible for other jurisdictions, but the tier structure could be a solid compromise to balance academic freedom with security measures. This approach would also allow for nuanced engagement, mitigating risks without broadly restricting international cooperation.
3. Restrict Access to Sensitive Research Facilities: Utilize the tiered system to manage physical access to specific research facilities rather than imposing blanket visa restrictions on students and researchers from particular countries. This strategy minimizes profiling and focuses on securing critical infrastructure, ensuring that access is granted based on security assessments related to specific research areas.
4. Establish a Fund for Capacity-Building Initiatives: Under the joint leadership of national security agencies and educational ministries, create a fund to support professional associations and academic unions. This fund would enhance their understanding of the security implications of their work and empower them to develop actionable policy recommendations. Such bottom-up initiatives can foster broader acceptance of top-down security measures and promote a culture of shared responsibility in safeguarding research integrity.

By adopting these policies, countries can develop research security frameworks that protect national interests while promoting international collaboration and academic freedom.

Bibliography

Chen, Yu-fu and William Hetherington. "Security Act Amendments Need to Be Enacted: TSP." *Taipei Times*, August 17, 2023. https://www.taipeitimes.com/News/taiwan/archives/2023/08/17/2003804868.

Doublethink Lab. "CITW 2023 in Taipei: Uniting to Counter Evolving PRC Threats." *Medium*, July 10, 2024. https://medium.com/doublethinklab/citw-2023-in-taipei-uniting-to-counter-evolving-prc-threats-e5ea4fdbecb8.

Diamond, Larry, James O. Ellis and Orville Schell, eds. *Silicon Triangle: The United States, Taiwan, China, and Global Semiconductor Security*. Hoover Institution Press, 2023.

d'Hooghe, Ingrid and Jonas Lammertink. *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Center, November 2022. https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safequard-Knowledge-Development-in-Science-and-Technology.pdf.

Freedom House. "Taiwan." *Freedom in the World*. Accessed November 21, 2024. https://freedomhouse.org/country/taiwan.

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), and the V-Dem Institute. "Academic Freedom Index." 2024. https://academic-freedom-index.net/.

Hsieh, Brian Hsiang-Yang and Henry Jin-Han Hsieh. "Amended National Security Act Imposes Stricter Punishments on Trade Secret Misappropriation Following New List of Crucial Tech." *IAM Media*, January 17, 2024. https://www.iam-media.com/article/amended-national-security-act-imposes-stricter-punishments-trade-secret-misappropriation-following-new-list-of-crucial-tech.

Ho, Ming-sho. *Challenging Beijing's Mandate of Heaven: Taiwan's Sunflower Movement and Hong Kong's Umbrella Movement*. Temple University Press, 2019.

Ho, Ming-sho and Thung-hong Lin. "The Power of Sunflower: The Origin and the Impact of Taiwan's Protest against Free Trade with China." In *The Umbrella Movement*, edited by Ming-sho Ho and Thung-hong Lin. Amsterdam University Press, 2017. https://doi.org/10.1515/9789048535248-013.

Huang, Jaw-Nian. "China's Influence on Taiwan's Media: A Model of Transnational Diffusion of Chinese Censorship." In *China's Influence and the Center-Peri-*

phery Tug of War in Hong Kong, Taiwan and Indo-Pacific, edited by Brian C. H. Fong, Jieh-min Wu and Andrew J. Nathan, 205–223. Routledge, 2020. https://doi.org/10.4324/9781003088431-17.

Huang, Mei-chu and Fion Khan. "Thirty Locations Raided in Talent, Tech Poaching Investigations." *Taipei Times*, September 3, 2024. https://www.taipeitimes.com/News/taiwan/archives/2024/09/03/2003823210.

Huntington, Samuel. "Democracy's Third Wave." *Journal of Democracy* 2, no. 2 (1991): 12–34.

InvesTaiwan. "Three Major Programs for Investing in Taiwan." 2024. https://investtaiwan.nat.gov.tw/showPageeng1135?lang=eng&search=1135.

Janda, Jakub, Marcin Jerzewski, Zuzana Košková and David Toman. *Fortifying Economic Security: The EU's Response to China's Risk*. Wilfried Martens Centre for European Studies, June 17, 2024. https://www.martenscentre.eu/publication/fortifying-economic-security-the-eus-response-to-chinas-risk/.

Jennings, Ralph. "For Mainland Chinese Students, Taiwan's Universities Are 'like Paradise.' But There's a Catch." *Los Angeles Times*, March 26, 2017. https://www.latimes.com/world/asia/la-fg-taiwan-china-students-2017-story.html.

Kumara, Ajantha Sisira and Ramanie Samaratunge. "The Effect of Academic Freedom on Electoral Democracy in the Asian Region." *Public Administration and Development* 44, no. 3 (2024): 137–149.

Lee, Tzu-I. "Bordering Secrecy: An Empirical Study on Cross-Border Trade Secret Misappropriation in the Semiconductor Sector." *Connecticut Journal of International Law* 39, no. 2 (June 30, 2024): 166–237. https://ssrn.com/abstract=4827530.

Lin, Ying-Yu. "China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures." *Taiwan Strategists*, no. 20 (2023): 37–54.

Liu, Shih-chung. "The Impact of U.S.-China Trade Friction on Both Countries and the Global Economy." P*rospects & Perspectives*, no. 8 (2018): 1–4. https://www.pf.org.tw/tw/pfch/33-7901.html.

Martin Purbrick. *United Front Work and Beyond: How the Chinese Communist Party Penetrates the United States and Western Societies*. Jamestown Foundation, April 12, 2023. https://jamestown.org/wp-content/uploads/2023/04/United

-Front-Work-and-Beyond_How-the-Chinese-Communist-Party-Penetrates-the-United-States-and-Western-Societies.pdf

ROC (Taiwan) Mainland Affairs Council. *Executive Yuan Approves the "Draft Amendments to Part of the Provisions of the Act Governing Relations between the People of the Taiwan Area and the Mainland Area."* February 17, 2022. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&sms=E828F60C4AFBAF90&s=6A543758F2225F94.

ROC (Taiwan) National Science and Technology Council. 政府資助 國家核心科技 研究計畫 安全管制作業手冊 (Government-Funded National Core Science and Technology Research Program Safety Control Operation Manual). January 2023.

ROC (Taiwan) National Science and Technology Council. 國家核心關鍵技術項目及其技術主管機關修正草案 (National Key Critical Technologies and Their Governing Authorities - Revised Draft). November 1, 2024.

Rigger, Shelley. *The Tiger Leading the Dragon: How Taiwan Propelled China's Economic Rise*. Stanford University Press, 2020.

Wang, Yu-Li and Luc Chia-Shin Lin. "Is Involvement Effective? A Case Study of Exchange Programs' Influence on Mainland Chinese Communications Major Exchange Students' Support for Taiwan." *Journal of Studies in International Education* 27, no. 2 (2023): 316–335. https://doi.org/10.1177/10283153211031042.

Wæver, Ole. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz, 46–86. Columbia University Press, 1995. https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf.

Weaver-Lee, Zoë. "Taiwan's Companies Look Beyond China, but Key Challenges Remain." *Global Taiwan Brief* 8, no. 18 (2023): 12–14. https://globaltaiwan.org/wp-content/uploads/2023/09/GTB-8.18-PDF-Final.pdf.

Yang, Alan Hao. "Strategizing Taiwan's New Southbound Policy by the Practice of PPPP Configuration." *Journal of Contemporary East Asia Studies* 10, no. 1 (2023): 45–62.

PART IV.

KNOWLEDGE SECURITY AND RESEARCH ETHICS

https://doi org/10 59862/k7m2x9q4r8/13

Chapter 13

Addressing Disinformation Vulnerabilities in International Students and Paths to Resilience

ELIZA KOTOWSKA

ORCID 0009-0000-5035-0541

Abstract: International students face particular vulnerabilities to disinformation due to unique social and digital factors associated with adjusting to a new country. They often rely on social media to obtain information about their host country and maintain connections with loved ones back home, which can increase their susceptibility to false narratives and disinformation. Furthermore, a lack of familiarity with local infor mation ecosystems, language barriers, and a strong need for social acceptance make them potential targets for disinformation campaigns. This heightened susceptibility underscores the need for tailored media literacy programs. By fostering critical thinking skills and enhancing awareness of disinformation tactics, educational institutions can play a crucial role in equipping international students with the resilience required to safely navigate today's complex information landscape.

Keywords: Social media, language barriers, political context, media literacy, social inclusion

Introduction

Disinformation represents a deliberate effort to manipulate public opinions and behaviors by disseminating misleading or false information, often crafted to spread rapidly within social networks. Its effectiveness lies in a combination of psychological vulnerabilities, societal dynamics, and information ecosystems. Disinformation targets human emotions and exploits our need for social connection and validation. Narratives are designed to evoke intense emotional reactions—such as anger, fear, or outrage—and prompt individuals to share them within their networks. This sharing creates echo chambers, where individuals reinforce one another's existing beliefs and over time, create closed information loops which amplify biases and diminish exposure to diverse perspectives. Furthermore, algorithms on digital platforms are designed to prioritize engagement, often promoting content similar to what users have previously interacted with, regardless of its accuracy and credibility.[1] This cycle perpetuates the spread of disinformation, embedding falsehoods into public discourse and personal belief systems.

Disinformation operates in such a way that virtually no one is entirely immune to its influence. By exploiting human psychology and the dynamics of information ecosystems, it ensures the rapid spread of false narratives. However, resilience to disinformation can be built through media literacy, critical thinking, and a solid understanding of current events. Media literacy empowers individuals to critically assess information and engage thoughtfully with content. In the realm of political disinformation, awareness of the political landscape is essential for recognizing the motivations behind manipulative campaigns, allowing individuals to evaluate who benefits from specific narratives and why. This awareness also enhances the ability to detect bias and manipulation, making individuals less susceptible to emotionally charged content designed to sway public opinion.

Despite these protective factors, certain groups remain more vulnerable to disinformation. For instance, research indicates that while older generations often perceive themselves as more susceptible to misinformation, younger people are generally more adept at identifying disinformation, thanks to practices such as "lateral reading" and fact-checking.[2] However, other stu-

[1] Donghee Shin, Michael Hameleers, Yong Jin Park, Jeong Nam Kim, Daniel Trielli, Nicholas Diakopoulos, Natali Helberger, Seth C. Lewis, Oscar Westlund and Sabine Baumann, "Countering Algorithmic Bias and Disinformation and Effectively Harnessing the Power of AI in Media," *Journalism & Mass Communication Quarterly* 99, no. 4 (2022): 887–907.

[2] "A Global Study on Information Literacy," Poynter Institute, August 2022, https://www.poynter.org/wp-content/uploads/2022/08/A-Global-Study-on-Information-Literacy-1.pdf.

dies, such as the one conducted by the University of Cambridge, suggest that younger adults may actually be worse at recognizing false political headlines than older adults.[3] This particular study showed that younger participants struggled more to identify misleading political content. These findings suggest that resilience against disinformation is not necessarily linked to age or familiarity with the internet but rather to media literacy and an understanding of the political context. Hence, even young individuals who might be familiar with technology, but lack exposure to media literacy education and are unfamiliar with the political landscape, are at a disadvantage. Additionally, social dynamics play a significant role in the spread of disinformation. Studies have shown a positive correlation between socialization and the sharing of misleading information.[4] In other words, people often share disinformation in pursuit of social validation.[5] As a result, those who are socially isolated may be more prone to disseminating disinformation, or in this case misinformation as they might not be aware that it is false, in hope of social inclusion.

The factors outlined above represent just a few of the challenges international students face when encountering disinformation in their host countries. Their potential social isolation and desire for social inclusion heighten their vulnerability to misleading narratives. Furthermore, unfamiliarity with the political context of their host country complicates their ability to identify politically charged disinformation. Students from countries with limited media freedom or low levels of media literacy may also struggle to discern credible news sources, leaving them more susceptible to manipulation. The language barrier further exacerbates these risks, as it may prevent them from fully understanding or critically engaging with the information they encounter. The following section will delve deeper into these factors, before offering recommendations for fostering resilience against disinformation.

[3] Fred Lewsey, "Misinformation Susceptibility Test," *University of Cambridge*, June 29, 2023, https://www.cam.ac.uk/stories/misinformation-susceptibility-test.

[4] Yanqing Sun and Juan Xie, "Who shares misinformation on social media? A meta-analysis of individual traits related to misinformation sharing," *Computers in Human Behavior* 158 (2024): 108–271.

[5] Barui K. Waruwu, Edson C. Tandoc, Jr, Andrew Duffy, Nuri Kim and Rich Ling, "Telling lies together? Sharing news as a form of social authentication," *New Media & Society* 23, no. 9 (2021): 2516–2533.

Disinformation Vulnerabilities in International Students

Social media has become a prominent platform for the dissemination of disinformation. Studies have shown that we pay more attention to news which create intense emotions[6] and are more likely to believe news which evoke fear and outrage.[7] Since disinformation exploits societal vulnerabilities and ongoing controversial debates while utilizing strong emotions of fear and anger, it is not surprising that these narratives appear in our social media.[8] This poses a problem for international students because social media is a crucial tool for them to maintain contact with their families and friends back home. Therefore, the likelihood that they will be exposed to disinformation increases significantly, given the amount of time they will likely spend on social media. Furthermore, studies have shown that we are more likely to believe a message to which we have been frequently exposed.[9] Therefore, the frequent engagement of international students with disinformation ridden social media heightens their exposure and vulnerability to disinformation.

Moreover, the new and maybe unfamiliar political setting and language, only heightens these individuals' susceptibility to disinformation narratives. When arriving in a new country, these students can often lack a deep understanding of the political landscape, the current debates, and public opinions. Without this background knowledge, it might be difficult to critically analyze politically charged information. Furthermore, the unfamiliarity with the information ecosystem, can also make it harder to distinguish between credible and biased news sources, as they can be unfamiliar with the local news. Additionally, some students may come from countries where there is little to no freedom of media and therefore might be unfamiliar with independent

[6] Megan McBride, Heather Wolters, Kaia Haney, William Rosenau, Neil Carey and Kasey Stricklin, The Psychology of (Dis) information: *Case Studies and Implications*, (Center for Naval Analyses, 2021), https://apps.dtic.mil/sti/trecms/pdf/AD1181768.pdf.

[7] "Journalism and Facts: Misinformation, Belief, and Action," *American Psychological Association*, November 29, 2023, https://www.apa.org/topics/journalism-facts/misinformation-belief-action.

[8] Massimo Flore, "Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives," *European Commission,* (2020).

[9] Madeline Jalbert, Eryn Newman and Norbert Schwarz, "Only Half of What I'll Tell You Is True: Expecting to Encounter Falsehoods Reduces Illusory Truth," *Journal of Applied Research in Memory and Cognition* 9, no. 4 (2020): 602–613.

media as they have been taught to rely on only government messaging. This can create a significant problem in navigating a new information ecosystem, where information and news are spread by both governments and independent media. Moreover, due to the language barrier, students might rely on their home news for information. In the case that their country's government does control the media, it means that their access to multidimensional media is limited, and they might be exposed to information about their host country, which they cannot verify locally. Although not every international student will come from countries where the media is state controlled, nevertheless, a new information ecosystem, unfamiliarity with news sources, and the language barrier might pose significant obstacles to finding credible information.

Social dynamics play another key role in international students' vulnerability to disinformation. Due to cultural or language barriers, international students might have a harder time making friends. Hence, if a student feels isolated in their new environment, they might reach for online connections. While this practice is not inherently harmful, there exists a correlation between social inclusion and the spread of false information online.[10] In order to bond with their peers, they might share similar content in hope of strengthening the bond. Afterall, we are more likely to engage with individuals who share similar interests.[11] However, due to the previously mentioned factors, such as unfamiliarity with the information ecosystem and the language barrier, they might be unable to critically engage with the information in order to verify its credibility and unknowingly spread false information. Furthermore, as people are more likely to share disinformation if it comes from a trusted source, or someone with whom they feel a sense of common identity, it is likely that they might engage with disinformation if it comes from peers with whom they have just bonded or are hoping to get

[10] Jingwen Zhang, Wen Wang and Jason A. Martin, "The Role of Social Media Literacy in Reducing Belief in COVID-19 Misinformation and Conspiracy Theories," *Computers in Human Behavior* 150 (2024).

[11] Gustavo Mesch and Ilan Talmud, "The Quality of Online and Offline Relationships: The Role of Multiplexity and Duration of Social Relationship," *The information society* 22, no. 3 (2006): 137–148.

to know.[12] Therefore, in the pursuit of that social inclusion, international students might become more likely to spread misinformation.

The aforementioned factors are only a fraction of the vulnerabilities which make international students more susceptible to disinformation. Their trust or mistrust towards media influenced by their home countries, the targeting of specific disinformation actors, and the many other challenges which come along with adapting to a new culture, can have a strong influence on their resilience to disinformation. Understanding these factors, however, is key to developing strategies to mitigate the spread of disinformation and enhancing collective resilience.

Paths to Resilience

There is no single way to combat disinformation. However, most literature and recommendations focus on media literacy. Media literacy is crucial in the fight against disinformation and must remain an important tool. While it should start during the early stages of education, it should also be a lifelong effort. Evolving technology, such as AI, continuously makes disinformation harder to recognize. Hence, media literacy must evolve with it and include new methods of recognizing disinformation. This is especially important for international students, as access to media literacy education may not be available in every country and can therefore vary significantly among individuals in this group. Universities should create workshops, if not lectures, on media literacy which are open to both local and international students. Higher education requires students to critically engage with information on a daily basis and therefore, offering assistance with media literacy skills will not only help students strengthen their resilience against disinformation, but will also benefit them during their academic journey.

One of the factors which make international students more susceptible to disinformation, is the lack of political and social context of the country. While it

[12] Tom Buchanan and Vladlena Benson, "Spreading Disinformation on Facebook: Do Trust in Message Source, Risk Propensity, or Personality Affect the Organic Reach of 'Fake News'?" *Social media+ society* 5, no. 4 (2019); Karen Hao, "Gen Z Is the Most Vulnerable Generation to Online Misinformation," *MIT Technology Review*, June 30, 2021, https://www.technologyreview.com/2021/06/30/1026338/gen-z-online-misinformation/.

might be too unrealistic to expect universities to educate all their international students on the entire history of the host country, it would be beneficial to bring students closer to the culture. By creating social events which allow international students to mingle with local students, the university is providing students with an opportunity to learn about the country from individuals who actually live there. Local students will have a chance to share the political, social, and cultural context of the host country which can help international students get more familiar with their environment. This can help students critically engage with information, as they will have a better understanding and background of the current situation. In fact, these interactions can help international students overcome multiple challenges which might be negatively affecting their resilience.

Social events can provide international students with the opportunity to form new friendships and bonds, and create a sense of belonging and social inclusion. These connections can help reduce students' anxiety about feeling socially excluded and discourage them from sharing content they're unsure about just to gain social validation from their peers. Friendships and regular interaction with local students can also help with the language barrier, as it provides them with someone who can help them navigate through the foreign language.

It is important to acknowledge the hardships which can make international students more susceptible to local disinformation. Social inclusivity and media literacy education are just two pathways which universities can utilize to help international students strengthen their resilience to disinformation. It is vital that universities take a multidimensional approach to this challenge by combining education, support, and social integration that can decrease the risks disinformation poses to this vulnerable group. By fostering a supportive and informed environment, universities can empower international students to critically engage with the information they encounter, ultimately reducing the spread and impact of disinformation.

Policy Recommendations

International students face a unique challenge in the fight against disinformation. Their frequent usage of social media platforms increases their exposure to disinformation narratives, while unfamiliarity with the host country's information ecosystem, and political context decreases their ability to critically analyze information. Unfamiliarity with the local language further exacerbates the issue, as it limits the number of news sources they have available for fact-checking and lateral reading. Furthermore, social isolation may prompt them to seek online connections, increasing their vulnerability to disinformation and the likelihood of inadvertently sharing misinformation. Universities should play a key role in creating an informed and supportive environment which can help increase international students' resilience to disinformation.

Recommendations

1. Universities should offer workshops or lectures on the fundamentals of media literacy, accessible to all students, as disinformation poses a universal threat. Some students may come from countries with low media literacy rates, and since critically engaging with information is a regular part of a student's curriculum, universities should offer courses which help students improve these skills.
2. Universities should supply information about credible news sources and where to find them. In today's digital age, there are so many news sources available online, it can be hard to distinguish between the credible and non-credible ones. This can be especially difficult for international students, who may not be familiar with the local information ecosystem. Providing a list of credible sources, in various languages, can help students navigate the information landscape. Furthermore, universities should ensure their students have access to these reliable news sources.
3. Universities should also provide a list of fact-checking resources, including websites of NGOs and organizations dedicated to this work. Collaboration between higher education institutions and fact-checking organizations offers mutual benefits: students and faculty gain access to valuable training and expertise, while fact-checking organizations enhance their visibility and reach within academic communities.
4. In collaboration with fact-checking organizations, universities can also monitor the media landscape to keep the student body informed abo-

ut the current disinformation trends and narratives likely targeting students and the community. Such information can be placed in a separate tab on the university's website or sent through the university's newsletter. By creating such initiatives, the university can invite students to become fact-checkers and provide training on fact-checking tools.

5. Extracurricular courses which provide an introduction to the politics, culture, and history of the host country should be arranged. By providing students with a deeper understanding of the country's political systems, media landscape, cultural norms, and historical events, they have a higher chance of recognizing when a piece of information or narrative is false.
6. Universities should organize social events which give an opportunity for international students to meet local students. These events can be in the form of cultural nights, collaborative projects, or community service initiatives. Helping international students integrate into the local community and form friendships can reduce social isolation, which might otherwise lead them to seek online connections and increase their exposure to disinformation. These friendships can also become reliable sources of information, which makes it less likely that individuals will seek information from less reliable sources online. Furthermore, local students can provide international individuals with insights into their information ecosystem as well as cultural, political, and historical contexts. Interactions with the local community can also break down stereotypes which disinformation campaigns often exploit.

Bibliography

"Journalism and Facts: Misinformation, Belief, and Action." American Psychological Association. November 29, 2023. https://www.apa.org/topics/journalism-facts/misinformation-belief-action.

Buchanan, Tom and Vladlena Benson. "Spreading Disinformation on Facebook: Do Trust in Message Source, Risk Propensity, or Personality Affect the Organic Reach of 'Fake News'?" *Social media+society 5*, no. 4 (2019): 2056305119888654.

Flore, Massimo. "Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives." *European Commission*, 2020.

Hao, Karen. "Gen Z Is the Most Vulnerable Generation to Online Misinformation." *MIT Technology Review*, June 30, 2021, https://www.technologyreview.com/2021/06/30/1026338/gen-z-online-misinformation/.

Jalbert, Madeline, Eryn Newman and Norbert Schwarz. "Only Half of What I'll Tell You Is True: Expecting to Encounter Falsehoods Reduces Illusory Truth." *Journal of Applied Research in Memory and Cognition* 9, no. 4 (2020): 602–613.

Karen, Hao. "Gen Z Is the Most Vulnerable Generation to Online Misinformation." *MIT Technology Review*. June 30, 2021. https://www.technologyreview.com/2021/06/30/1026338/gen-z-online-misinformation/.

Lewsey, Fred. "Misinformation Susceptibility Test." *University of Cambridge*. June 29, 2023. https://www.cam.ac.uk/stories/misinformation-susceptibility-test.

McBride, Megan, Heather Wolters, Kaia Haney, William Rosenau, Neil Carey and Kasey Stricklin. The Psychology of (Dis) information: *Case Studies and Implications*. Center for Naval Analyses, 2021. https://apps.dtic.mil/sti/trecms/pdf/AD1181768.pdf.

Mesch, Gustavo and Ilan Talmud. "The Quality of Online and Offline Relationships: The Role of Multiplexity and Duration of Social Relationship." *The information society* 22, no. 3 (2006): 137–148.

"A Global Study on Information Literacy." *Poynter Institute*. August 2022, https://www.poynter.org/wp-content/uploads/2022/08/A-Global-Study-on-Information-Literacy-1.pdf.

Shin, Donghee, Michael Hameleers, Yong Jin Park, Jeong Nam Kim, Daniel Trielli, Nicholas Diakopoulos, Natali Helberger, Seth C. Lewis, Oscar Westlund and Sabine Baumann. "Countering Algorithmic Bias and Disinformation and Effectively Harnessing the Power of AI in Media." *Journalism & Mass Communication Quarterly* 99, no. 4 (2022): 887–907.

Sun, Yanqing and Juan Xie, "Who shares misinformation on social media? A meta-analysis of individual traits related to misinformation sharing," *Computers in Human Behavior* 158 (2024): 108–271.

Waruwu, Barui K., Edson C. Tandoc, Jr, Andrew Duffy, Nuri Kim and Rich Ling. "Telling lies together? Sharing news as a form of social authentication." *New Media & Society* 23, no. 9 (2021): 2516–2533.

Zhang, Jingwen, Wen Wang and Jason A. Martin. "The Role of Social Media Literacy in Reducing Belief in COVID-19 Misinformation and Conspiracy Theories." *Computers in Human Behavior* 150 (2024).

https://doi org/10 59862/k7m2x9q4r8/14

Chapter 14

Knowledge Security: A New Policy Concept for Science and Politics

LEO EIGNER
Center for Security Studies (CSS), ETH Zurich

Abstract: The global science, technology, and innovation (STI) sector thrives on open exchange and international collaboration, yet it also underpins national economic and political competitiveness and can intensify geopolitical rivalries. In recent years, authoritarian governments have exploited the openness of the global STI sector to their advantage, creating significant security and ethical risks. To address these challenges, scientifically leading, democratic nations have developed the policy concept of knowledge security (or research security), which seeks to safeguard scientific values and assets as well as national security. This paper describes six overarching knowledge security risks faced by higher education institutions (HEIs) and research-performing organizations (RPOs) and highlights the divergent perspectives of science and policy actors. It outlines the emerging consensus on balancing openness with security and outlines diverse approaches and measures shaping knowledge security policy. The paper concludes with a description of seven guiding principles that can support the process of policy formulation and implementation.

Keywords: knowledge security; research security; science, technology, and innovation policy; strategic competition; security policy

Scientific and technological advancements result from the free exchange of ideas. For this reason, open science, academic mobility, and international cooperation are cornerstones of national science, technology, and innovation (STI) sectors, which collectively form a globally integrated STI sector. Because STI are perceived to lie at the heart of national competitiveness, higher education institutions (HEI) and other research performing organizations (RPO) inhabit a highly contested space where multiple actors vie for access and control of crucial STI assets and developments. To some extent, this has always been the case. Yet due to rising tensions between rival political systems and ideologies, this competition has reached new heights.

Over the past decades, certain autocratic countries, which have a broader interpretation of national security, have exploited the openness of the global STI sector to further their own agendas.1 The governments of China, Russia, Iran, and North Korea have, for instance, strengthened their military capabilities, expanded their repressive surveillance systems, deployed STI to suppress human rights domestically, and spread propaganda and self-censorship abroad.2 This poses security and ethical risks to scientific values and national interests in democratic, scientifically leading countries. For this reason, science and policy actors in Australia, Canada, the EU, EU Member States, Japan, Norway, Switzerland, Taiwan, the UK, and the US are currently formulating and implementing policies at institutional, national, and international level to tackle these security and ethical risks.3 These policies are generally referred to as knowledge security or research security.

The aim of knowledge security is to safeguard scientific values and practices as well as national security and interests.4 More specifically, it seeks to

[1] For country agnostic studies, see: Arena Baykal and Thorsten Brenner, "Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies," *Global Public Policy Institute*, October 22, 2020. For China related studies, see: Ingrid D'Hooghe et al., "Assessing Europe-China Collaboration in Higher Education and Research," *Leiden Asia Centre*, 2018; Rebecca Arcesati, Irène Hors and Sylvia Schwargg Serger, "Sharpening Europe's approach to engagement with China on science, technology and innovation," *MERICS*, December 2021.

[2] For military related topics, see: Alex Joske, "Picking flowers, making honey: The Chinese military's collaboration with foreign universities," *Australian Strategic Policy Institute*, October 30, 2018. For surveillance and human rights related reports, see: Yves Moreau, "Crackdown on genomic surveillance," *Nature*, December 5, 2019, https://www.nature.com/articles/d41586-019-03687-x; Billy Perrigo, "Exclusive: Workers at Google DeepMind Push Company to Drop Military Contracts," *Time Magazine*, August 23, 2024, https://time.com/7013685/google-ai-deepmind-military-contracts-israel/. For propaganda related studies, see: Clive Hamilton and Mareike Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World* (Oneworld Publications, 2020).

[3] For an over of national policies, see: Ingrid D'Hooghe and Jonas Lammertink, "How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology," *Leiden Asia Centre*, November 2022.

[4] Leo Eigner, "Knowledge Security at Stake," *CSS Analyses in Security Policy*, no. 336 (2024).

address six overarching risks: (1) preventing the transfer of sensitive knowledge and technology to actors involved in human rights violations and/or foreign military and security systems; (2) mitigating infringements of scientific integrity and scientific values, such as academic freedom and institutional autonomy; (3) ensuring reciprocity and transparency with international partners; (4) avoiding science monopolies and financial dependencies on international partners; (5) avoiding discriminatory knowledge security policies and a hard decoupling; and (6) preventing loopholes and asymmetrical implementation of knowledge security policies.5 In short, knowledge security seeks to "derisk" and to "decouple" national STI sectors from the global STI sector. Knowledge security thus represents a new intersectional policy concept that, like economic or energy security, grapples with a much larger concern, namely, how to engage in strategic competition in a highly interconnected world.

Since the late 2010s, science and policy actors in the above-mentioned countries have debated how best to address knowledge security risks. While most stakeholders agree that neither a completely open nor a completely closed STI sector is desirable, opinions differ as to the degree to which the STI sector can and should be open or closed. A free and open STI sector would risk perpetuating its exploitation as well as the long-term erosion of scientific values and national security. By contrast, a secure and closed STI sector would harm international relations and scientific partnerships. It could also curtail the free exchange of ideas and cut science actors from accessing important STI developments, talent, infrastructure, and capital from abroad. The answer, then, is to find a balanced, proportionate approach that preserves scientific excellence, values, and exchange while ensuring safety and security of the STI sector and the nation's interests at large.[6]

[5] Leo Eigner, "Knowledge Security: Ein neues Konzept für die Schweiz," *Bulletin 2024 zur schweizerischen Sicherheitspolitik* (Center for Security Studies, 2024), 111–138.

[6] This view is widely expressed by science as well as policy actors: "Die akademische Zusammenarbeit mit China realistisch gestalten," *DAAD*, January 4, 2024); Irna van der Molen et al., "Keeping science open? Current challenges in the day-to-day reality of universities, *CESAER*, October 18, 2023; "Integrity and Security in the Global Research Ecosystem." *OECD*, June 22, 2022; Tommy Shih, "We cannot adopt a blanket approach to research security," *University World News*, October 2, 2024, https://www.universityworldnews.com/post.php?story=20241001140316637.

However, science and policy actors often have different perspectives on this balancing act. Policy actors, such as bureaucrats, government agencies, and parliamentarians, generally believe that knowledge is power and a national asset. To them, STI are a source of national prosperity, competitiveness, and security that should be preserved in the nation's interests. By contrast, science actors, such as individual researchers, funding agencies, and HEI, generally believe that knowledge is free and a global public good. To them, this is primarily a matter of practice, as scientific excellence results from international exchange and mobility. At the same time, it is also a principle, as knowledge cannot be owned and therefore belongs to everyone. In addition, science actors are often wary of knowledge security, because they fear domestic political interference or prescriptive policymaking that may infringe on their academic freedom—a law in many scientifically leading, democratic countries—and the institutional autonomy of their home organizations.[7] This divergent, epistemic interpretation of STI and its role in society can pose difficulties when formulating national knowledge security policies.

Since the late 2010s, when the awareness for knowledge security risks rose among various science and policy communities, international consensus on how best to address these risks has grown.[8] For instance, there is a broad agreement regarding the distribution of roles and responsibilities. Science actors, particularly individual researchers and their home organizations, are considered to be responsible for implementing knowledge security policies. This safeguards their academic freedom and institutional autonomy and thus ensures the legitimacy of knowledge security policies. However, if science actors implement measures on their own, this could create loopholes that foreign actors can exploit. Cooperation with policy actors is therefore essential. Generally speaking, policy actors are assigned supportive and

[7] This UK example illustrates a common fear among science actors: John Morgan, "Red tape warning for research projects over national security law," *Times Higher Education*, February 17, 2022, https://www.timeshighereducation.com/news/red-tape-warning-research-projects-over-national-security-law.

[8] A recent survey found that science actors spend more time on knowledge security issues: Mark Hahnel, Simon Porter and Rachael Delevante, "Research Transformation: Change in the era of AI, open and impact," *Digital Sciences*, October 28, 2024.

coordinating responsibilities. Ideally, they provide science actors with advice and expertise on security and foreign policy, financial and intelligence resources, and sound legal frameworks that empower science actors to act according to their mandates, needs, and functions. Due to the complexity of knowledge security risks and policies, coordination is widely considered a joint responsibility.

Consensus is also forming around the general approach to knowledge security. Following pushback from science communities against top-down and prescriptive approaches in countries such as Australia, Canada, and the US, governments are increasingly adopting a more bottom-up approach geared towards supporting science actors in the formulation and implementation of knowledge security policies.[9] In this respect, the Netherlands has become something of a blueprint for sound knowledge security policy. Not only were Dutch science and policy actors early to respond to knowledge security risks; their experience in the formulation and implementation of knowledge security policies exemplifies a process of common threat representation, information gathering and exchange, stakeholder assemblage, role allocation, and coordination within and between their national science and policy communities.[10] As a result, Dutch actors have influenced international standards when it comes to knowledge security policies, particularly within Europe and the EU.

When it comes to concrete measures, however, there is no national nor international consensus. Instead, there are a broad range of measures taken at institutional and national level that vary in their scope and latitude. Institutional measures include: raising awareness for knowledge security through educational programs; reviewing codes of conduct and ethical review processes; screening individual researchers in "sensitive" areas and

[9] For pushback against top-down policymaking, see: Richard L. Hudson, "Canada tightens security for university research, affecting ties to China," *Science* | *Business*, January 18, 2024, https://sciencebusiness.net/news/international-news/canada-tightens-security-university-research-affecting-ties-china; Richard L. Hudson, "Pentagon advisors urge caution in tightening science security," Science | Business, March 22, 2024, https://sciencebusiness.net/news/international-news/pentagon-advisors-urge-caution-tightening-science-security.

[10] David Snetselaar, "DREAMS Lab: Assembling knowledge security in Sino-Dutch research collaborations," *European Security* 32, no. 2 (2023), 233–251.

with certain scholarships for links to foreign military and security apparatuses[11] screening foreign investment in projects, research centers, HEI, and RPO designed to shape public opinion and spread propaganda;[12] screening collaborations, programs, and partnerships with HEI, RPO, and companies for human rights abuses and/or links to foreign military and security apparatuses;[13] establishing compliance offices and implementing national and international export control regulations. National measures include: raising awareness among HEI and RPO through intelligence sharing and support;[14] establishing working groups and issuing non-binding knowledge security guidelines and strategies;[15] establishing national support structures for HEI, RPO, and companies;[16] providing funds to HEI and RPO to implement knowledge security policies;[17] reviewing and amending laws and regulations to provide a sound legal basis for knowledge security po-

[11] Yojana Sharma, "ETH foreign student screening leans on West's sanctions list," *World University News*, November 7, 2024, https://www.universityworldnews.com/post.php?story=20241107142108558; Yojana Sharma, "German university ends ties with China scholarship scheme," World University News, July 20, 2023, https://www.universityworldnews.com/post.php?story=20230720113914406.

[12] Bonnie Girard, "The Rise and Fall of Confucius Institutes in the US," *The Diplomat*, November 28, 2023, https://thediplomat.com/2023/11/the-rise-and-fall-of-confucius-institutes-in-the-us/.

[13] Examples on collaborations with Russia, China, and Israel: Richard Stone, "Western nations cut ties with Russian science, even as some projects try to remain neutral," *Science*, March 8, 2022, https://www.science.org/content/article/western-nations-cut-ties-russian-science-even-some-projects-try-remain-neutral; Pieter Haeck, "Belgian research powerhouse turns hawkish on China," *Politico*, April 4, 2024, https://www.politico.eu/article/belgium-university-town-leuven-reposition-protectionist-world-trade-technology-council/; David Matthews, "Academic boycotts over Gaza war jeopardise Israel's place in Horizon Europe," *Science | Business*, May 23, 2024, https://sciencebusiness.net/news/universities/academic-boycotts-over-gaza-war-jeopardise-israels-place-horizon-europe.

[14] Chris Havergal, "Security vetting plan for researchers of sensitive technologies," *Times Higher Education*, April 26, 2024, https://www.timeshighereducation.com/news/security-vetting-plan-researchers-sensitive-technologies.

[15] For a (slightly outdated) overview of national guidelines, see: D'Hooghe and Lammertink, "Safeguard Knowledge Development in Science and Technology."

[16] For example: the National Contact Point for Knowledge Security in the Netherlands, the Research Collaboration Advice Team (RMAT) in the UK, or the planned center, Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE), in the US.

[17] For example, the Canadian government has created a fund worth £75 million for five years. The UK is contemplating a similar approach: Jack Grove, "Russell Group urges creation of UK research security fund," *Times Higher Education*, October 17, 2023, https://www.timeshighereducation.com/news/russell-group-urges-creation-uk-research-security-fund.

licies;[18] initiating counter-espionage programs;[19] and expanding sanctions lists and export control regimes.

Knowledge security policies require alignment between science and policy actors. Seven principles—intrinsic to knowledge security and thus unavoidable—can help to guide stakeholders towards achieving this alignment.[20] First, national laws, such as academic freedom or the state's responsibility for national security, must be asserted. Determining which laws take precedence depends on the context and requires consultation among stakeholders. Second, knowledge security is a political issue rather than a scientific one, necessitating policies that balance national laws with international scientific norms and practices. Third, security and ethics are deeply interconnected aspects of knowledge security. As the STI sector becomes more securitized, a corresponding ethicalization of national security will take place. Fourth, knowledge security risks are complex. They are highly granular and constantly evolve, making them difficult to detect and monitor. Fifth, targeted interventions guided by a precautionary approach can address the inherent complexity of knowledge security risks. Sixth, knowledge security is a shared responsibility, relying on both collective efforts and individual accountability. Seventh, knowledge security is rooted in established norms, aims, and policies. It seeks to preserve open science, academic mobility, and international collaboration while ensuring these activities remain safe, fair, and secure.

The risks and policies of knowledge security represent a profound, long-term challenge to the core principles upon which the global STI sector is built. It is possible that the global STI sector may become less global and fragment into blocks that continue to interact, but in a far more pointed and risk-aware manner. While knowledge security represents a challenge, it is an

[18] In the UK, the Higher Education (Freedom of Speech) Act 2023 mandated the Office for Students, a regulator, to monitor HEI's dependence on foreign funding: Tom Williams, "Zahawi wants OfS to audit foreign donations for free speech risk," *Times Higher Education*, June 7, 2022, https://www.timeshighereducation.com/news/zahawi-wants-ofs-audit-foreign-donations-free-speech-risk.

[19] Natascha Gilbert, "China Initiative's shadow looms large for US scientists," *Nature*, February 23, 2024, https://www.nature.com/articles/d41586-023-00543-x.

[20] Eigner, "Knowledge Security," 133–136.

opportunity. It can prioritize relations between certain countries, expand the science-policy interface, and reinvigorate science diplomacy in crucial areas addressing global challenges.

Policy Recommendations

1. Adopt a balanced and precautionary approach to knowledge security to continue to promote international scientific collaboration.
2. Foster inclusive, consensus-driven knowledge security policy development between the science and policy communities at inter-institutional, national, and international level.
3. Ensure targeted, coherent, and consistent knowledge security policies that are in line with academic freedom and national security.

Bibliography

Arcesati, Rebecca, Irène Hors and Sylvia Schwargg Serger. "Sharpening Europe's approach to engagement with China on science, technology and innovation." *MERICS*, December 2021.

Baykal, Arena and Thorsten Brenner. "Risky Business: Rethinking Research Cooperation and Exchange with Non-Democracies." *Global Public Policy Institute*, October 2020.

D'Hooghe, Ingrid et al. "Assessing Europe-China Collaboration in Higher Education and Research." *Leiden Asia Centre*, 2018.

D'Hooghe, Ingrid and Jonas Lammertink. "How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology." *Leiden Asia Centre*, November 2022.

"Die akademische Zusammenarbeit mit China realistisch gestalten." *DAAD*, January 4, 2024.

Eigner, Leo. "Knowledge Security at Stake." *CSS Analyses in Security Policy*, no. 336 (2024).

Eigner, Leo. "Knowledge Security: Ein neues Konzept für die Schweiz." *Bulletin 2024 zur schweizerischen Sicherheitspolitik* (Center for Security Studies, 2024), 111–138.

Gilbert, Natascha. "China Initiative's shadow looms large for US scientists." *Nature*, February 23, 2024, https://www.nature.com/articles/d41586-023-00543-x.

Girard, Bonnie. "The Rise and Fall of Confucius Institutes in the US." *The Diplomat*, November 28, 2023, https://thediplomat.com/2023/11/the-rise-and-fall-of-confucius-institutes-in-the-us/.

Grove, Jack. "Russell Group urges creation of UK research security fund." *Times Higher Education*, October 17, 2023, https://www.timeshighereducation.com/news/russell-group-urges-creation-uk-research-security-fund.

Pieter Haeck. "Belgian research powerhouse turns hawkish on China." *Politico*, April 4, 2024, https://www.politico.eu/article/belgium-university-town-leuven-reposition-protectionist-world-trade-technology-council/.

Hahnel, Mark, Simon Porter and Rachael Delevante. *Research Transformation: Change in the era of AI, open and impact* (Digital Sciences, 2024).

Hamilton, Clive and Mareike Ohlberg. *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World* (Oneworld Publications, 2020).

Havergal, Chris. "Security vetting plan for researchers of sensitive technologies." *Times Higher Education*, April 26, 2024, https://www.timeshighereducation.com/news/security-vetting-plan-researchers-sensitive-technologies.

Hudson, Richard L. "Canada tightens security for university research, affecting ties to China." *Science | Business*, January 18, 2024, https://sciencebusiness.net/news/international-news/canada-tightens-security-university-research-affecting-ties-china.

Hudson, Richard L. "Pentagon advisors urge caution in tightening science security." *Science | Business*, March 22, 2024, https://sciencebusiness.net/news/international-news/pentagon-advisors-urge-caution-tightening-science-security.

"Integrity and Security in the Global Research Ecosystem." *OECD*, June 22, 2022.

Joske, Alex. "Picking flowers, making honey: The Chinese military's collaboration with foreign universities." *Australian Strategic Policy Institute*, October 30, 2018.

Matthews, David. "Academic boycotts over Gaza war jeopardise Israel's place in Horizon Europe." *Science | Business*, May 23, 2024, https://sciencebusiness.net/news/universities/academic-boycotts-over-gaza-war-jeopardise-israels-place-horizon-europe.

Moreau, Yves. “Crackdown on genomic surveillance.” *Nature*, December 5, 2019, https://www.nature.com/articles/d41586-019-03687-x.

Morgan, John. “Red tape warning for research projects over national security law.” *Times Higher Education*, February 17, 2022, https://www.timeshighereducation.com/news/red-tape-warning-research-projects-over-national-security-law.

Perrigo, Billy. “Exclusive: Workers at Google DeepMind Push Company to Drop Military Contracts.” *Time Magazine*, August 23, 2024, https://time.com/7013685/google-ai-deepmind-military-contracts-israel/.

Sharma, Yojana. “ETH foreign student screening leans on West’s sanctions list.” *World University News*, November 7, 2024, https://www.universityworldnews.com/post.php?story=20241107142108558; Sharma, Yojana. “German university ends ties with China scholarship scheme.” *World University News*, July 20, 2023, https://www.universityworldnews.com/post.php?story=20230720113914406.

Shih, Tommy. “We cannot adopt a blanket approach to research security.” *University World News*, October 2, 2024, https://www.universityworldnews.com/post.php?story=2024100114031663.

Snetselaar, David. “DREAMS Lab: Assembling knowledge security in Sino-Dutch research collaborations.” *European Security* 32, no. 2 (2023), 233–251.

Stone, Richard. “Western nations cut ties with Russian science, even as some projects try to remain neutral.” *Science*, March 8, 2022, https://www.science.org/content/article/western-nations-cut-ties-russian-science-even-some-projects-try-remain-neutral.

van der Molen, Irna et al. “Keeping science open? Current challenges in the day-to-day reality of universities.” *CESAER*, October 18, 2023.

Williams, Tom. “Zahawi wants OfS to audit foreign donations for free speech risk.” *Times Higher Education*, June 7, 2022, https://www.timeshighereducation.com/news/zahawi-wants-ofs-audit-foreign-donations-free-speech-risk.

https://doi org/10 59862/k7m2x9q4r8/15

Chapter 15

Decolonizing Knowledge: The Practical and Ethical Challenges of Researching “Sensitive” Topics in and about China

DAVID O’BRIEN
The Centre for International Studies and Development, Jagiellonian University
ORCID: orcid.org/0000-0002-9687-8736

Abstract: Much has been written about the need to decolonize knowledge and the western hegemony of scholarship. This in an important and continuing process that needs to take place. However, it is also the case that a similar and perhaps more restrictive hegemony exists in the People’s Republic of China today in the Xi Jinping era, where any position other that the position of the Communist Party cannot be expressed. This is not just restrictive it is also extremely dangerous for scholars working on what are considered highly sensitive topics such as Xinjiang and Tibet, especially ethnic minority scholars. Based on many years of working both as a teacher and researcher in China this paper seeks to understand this “decolonization” of knowledge as a multifaceted and complex process. In doing so it seeks to find a way in which scholars working both outside and within China can find a respectful and constructive way to engage in dialogue and debate. In seeking to explore the different power factors at play it will attempt to understand this process from multiple perspectives in an era in which scholarship is becoming ever more ideologized in both East and West.

Keywords: Chinese Communist Party, decolonization, securitization of knowledge, academic ethics

Much has been written about the need to decolonize knowledge and the western hegemony of scholarship. This in an important and continuing process that needs to take place. However, a similar and perhaps more restrictive hegemony exists in the People's Republic of China where any position other than the position of the Communist Party cannot be expressed. This is not just restrictive, it is also extremely dangerous for scholars working on what are considered highly sensitive topics such as Xinjiang and Tibet, especially for ethnic minority scholars.

Based on many years of working both as a teacher and researcher in China, this short paper seeks to understand "decolonization" of knowledge as a multifaceted and complex process. In doing so it seeks to find a way in which scholars working both outside and within China can find a respectful and constructive way to engage in dialogue and debate. In seeking to explore the different power factors at play, it will attempt to understand this process from multiple perspectives in an era in which scholarship is becoming ever more ideologized in both East and West.

Deimperialization (or decolonization) is an ongoing intellectual project.[1] It is an area of sometimes fierce debate within US and American academia. As Burawoy[2] describes it, "every university has been obliged to examine its past for collaboration with white supremacy, whether the university was constructed on land expropriated from indigenous people or from the proceeds of slavery, whether it consecrated propagators of racism in statutes, portraits or in the names of buildings." At times this debate has escalated into violence on campuses with statues being defaced, buildings vandalized, and speakers "deplatformed."

If we are to understand the decolonization of education as recognizing, critiquing, and expunging the presence of colonial presuppositions in canonical texts, then we also need to ask if this should only be limited to Western colonialism.[3] In taking China as an example, this short article attempts to

[1] Chen Kuan-Hsing, *Asia as Method: Toward Deimperialization* (Duke University Press, 2010), 257.

[2] Michael Burawoy, "Decolonizing Canons: A Conversation with Chinese Sociologists," in I*nterrogating the Future: Essays in Honour of David Fasenfest* (Brill, 2024), 98.

[3] Michael Burawoy, "Decolonizing Canons: A Conversation with Chinese Sociologists," in *Interrogating the Future: Essays in Honour of David Fasenfest* (Brill, 2024), 99.

explore whether this process could take place in our engagement with Chinese academia and scholars, or indeed whether such a process would lead to risks not just for academic freedom but also for the safety of researchers and students. This is a fundamental ethical issue for any of us working on topics that the Chinese Communist Party (CCP) consider sensitive or indeed teaching students from the People's Republic.

McMaugh et al.[4] argue that although there is a vast amount of discussion around "research ethics," this is at times delimited to "research" as data generation, rather than expanded to other aspects of academic work more broadly. They see all aspects of research as involving what they term "ethical labor": the reason why research is being done (motivation), how data is gathered (research methods), how research is represented (presentation), as well as how research is judged (review) and disseminated (impact), all entail questions of integrity. There is a vast amount of discussion on research ethics in research methods, and a fair amount on presentation (e.g., plagiarism), but seeing a far wider set of interconnected practices as likewise resting on ethical choices is uncommon but needed. Expanding the "ethics of research" beyond methods of gathering data draws attention to the ways in which numerous aspects of academic work entail complex forms of responsibility and questions of best practice.

To expand this still further, this is just as true of the academic environment of a university where teaching and research coexist. In this, university teaching is also "ethical labor," raising questions about: the reasons why such teaching is being done (the motivations of teachers and students), how teaching is done and how topics are represented (teaching techniques and content), how learning and teaching are evaluated (assessment), and ultimately the outcomes of the encounter, for students, teachers, and others.

I suggest that actively thinking about these aspects of one's teaching and research practice as ethical choices is a key means to bring the ethical labor of such work to the surface. This should be collaborative—these should be

[4] Anne McMaugh, Jennifer Sumsion, Colin Symes and David Saltmarsh, "From Ethics in Research to Ethics in Writing: Not Entirely Separate Matters," *Asia-Pacific Journal of Teacher Education* 34, no. 1 (2007): 1–3, https://doi.org/10.1080/13598660500481603.

things that are discussed among colleagues, even possibly in class. In this, I argue that such collaborative reflection should be a core part of "scholarly habitus,"[5] the norms of academic work that, ideally, become taken for granted. The ethical nature of both research and teaching is heightened in an authoritarian context where one must navigate one's responsibilities to students, colleagues, others, and oneself, where the stakes may be higher.

The idea that education is an ethical endeavor would in fact be familiar in China. In the Confucian tradition, education is regularly framed as the main means of "self-cultivation" through which one becomes a moral junzi (君子), "gentleman," or more gender-neutrally "ideal person."[6] This can also be seen as "citizen-making," "training so citizens fit a particular social, economic, and political order."[7] But the idea that education is a means of "becoming moral" for learners, or that education systems promote social norms, is not my point here. Instead, I am focusing upon the choices faced by researchers and teachers in such contexts, and the processes of reflection this entails for them.

A lot of academic debate around ethics in different cultural contexts is concerned with questions of the "universality" of ethical principles. While it is important to respect different cultural contexts, too much of this simplistically turns this into a debate between "Western" ethics focusing on "individuals" versus all others emphasizing "communities" or "family."[8] While growing out of valid postcolonial critique calling for the need to incorporate diverse viewpoints, the problem with such debates is that they accept and perpetuate binaries between "the West" and "the Rest," and often conflate

[5] Megan Watkins, "Discipline, Consciousness and the Formation of a Scholarly Habitus," *Continuum: Journal of Media & Cultural Studies* 19, no. 4 (2005): 545–557, https://doi.org/10.1080/10304310500322834.

[6] Jin Lin, "Rediscover Lasting Values: Confucian Cultural Learning Models in the Twenty-first Century," in *Re-envisioning Chinese Education: The Meaning of Person-making in a New Age* (Routledge, 2016), 130–147.

[7] David O'Brien and Melissa Shani Brown, *People, Place, Race and Nation in Xinjiang China: Territories of Identity* (Palgrave Macmillan, 2022).

[8] Bridget Pratt, Cassandra Van, Cong Yali, Harun Rashid, Nandini Kumar, Aasim Ahmed, Ross Upshur and Bebe Loff, "Perspectives from South and East Asia on Clinical and Research Ethics: A Literature Review," *Journal of Empirical Research on Human Research Ethics* 9, no. 2 (2004): 52–67, https://doi.org/10.1525/jer.2014.9.2.52.

rather than differentiate universal principles versus universal practices, or, as Czymoniewicz-Klippel, Brijnath, and Crockett[9] put it, the difference between "strategies and strictures." Most would agree that ethical paths are aimed at the avoidance of harm, but many disagree how this is best achieved.

In my own experience, the argument that China offers a "unique" or "exceptional" context where "Western values" are less applicable is often not a way of engaging in meaningful discussions about different cultures or different visions of ethical practice. Often, it was a way of using an assertion of cultural distinction to preclude discussion which was critical of Chinese politics in some way. The provision of a "Western education experience" which precludes "Western perspectives" is a logical impossibility, although it must also always consider context.

The hybrid space that is an intercultural classroom (and research environment) is made more dangerous when the repercussions of one's decisions could have a greater impact on those involved. When a class discussion could lead to one student reporting upon another, or presenting one's research could endanger the teacher/researcher or their collaborators, there are serious questions about when, or how, or even if, certain topics are broached. And yet, to pass over sensitive topics is also problematic: it contributes to students' ignorance of the world which is complicit in xenophobia and polarization.

Under Xi Jinping's leadership, China has become even more authoritarian. "Ideological and political education," or sixiang zhengzhi jiaoyu (思想政治教育), often shortened as sizheng (思政), is a subject taught in high schools and universities in China as part of the country's Patriotic Education Campaign (爱国主义教育) since the early 1990s.[10] Although training in ideology and correct political thinking have always been a part of the political culture of the CCP. According to Mao Zedong, "[G]etting to grips with the leadership of thought control is the first priority in maintaining overall leadership." In the words of Deng Xiaoping, "[D]uring the last ten years, our

[9] Melina Czymoniewicz-Klippel, Bianca Brijnath and Belina Crockett, "Ethics and the Promotion of Inclusiveness Within Qualitative Research: Case Examples From Asia and the Pacific," *Qualitative Inquiry* 16, no. 5 (2010): 332–341, https://doi.org/10.1177/1077800409358872.

[10] Stella Chen, "Ideological and Political Education," *The China Media Project*, December 17, 2001, https://chinamediaproject.org/the_ccp_dictionary/ideological-and-political-education/.

biggest mistake was made in the field of education, primarily in ideological and political education—not just of students but of the people in general." Jiang Zemin said that "the first thing for strengthening the party is to grasp ideological and political work, because solving ideological and political problems is the premise and foundation for other works." Hu Jintao argues that "ideology is an important front that we fiercely fight against hostile forces; if this front has some problems, it might lead to social turmoil and even the fall of our regime."[11]

Education then for the Communist Party is a part of the revolutionary war and students are the vanguard of this force. Almost all Chinese students are members of the Chinese Youth League, and many will go on to become full members of the Chinese Communist Party during their time as undergraduates. In 2016, 1.8 million students were Party members.[12] All Chinese students are required to undertake compulsory military training usually in their first year. Ideological and political education in China is aimed at "building a great socialist country and promoting relevant moral values in the conditions of the modern global world."[13]

In 2013, a list of topics on which teaching is specifically prohibited was issued, the so called "Seven Nos" of civil society, civil rights, universal values, legal independence, press freedom, the bourgeois class, and the historical wrongs of the Party.[14] So if none of this can even be discussed in the classroom how can we even engage with ideas of decolonization in our own classrooms with Chinese students. Can we discuss the situation of the Uyghur people or Tibetans without putting them at risk that their fellow Chinese students

[11] All quotations are taken from: Zeng Jinghan, "Ideological and Political Education in China," in *The Chinese Communist Party's Capacity to Rule. Critical Studies of the Asia-Pacific* (Palgrave Macmillan, 2016).

[12] Xu Liu, Zhao Xiantong and Hugh Starkey, "Ideological and Political Education in Chinese Universities: Structures and Practices," *Asia Pacific Journal of Education* 43, no. 2 (2023): 596–598, https://doi.org/10.1080/02188791.2021.1960484.

[13] Kequan Lin, "Chinese Ideology in the Political Education of Students: How Does Ideology-Based Teaching Impact Students' Consciousness?" *Journal of Knowledge Economy* (2024), https://doi.org/10.1007/s13132-024-02164-9.

[14] Tim Pringle and Sophia Woodman, "Between a Rock and a Hard Place: Academic Freedom in Globalising Chinese Universities," *The International Journal of Human Rights* 26, no. 10 (2022): 1782–1802, https://doi.org/10.1080/13642987.2022.2074979.

may report them (as has been documented)?[15] Might we need to reevaluate our syllabi? Publishers have been facing increasing demands to block content from publication "bundles" for sale in China. Such censorship is made possible by the "oligopoly" in academic publishing under which a handful of large global companies control the majority of publishing outlets, and these companies are becoming more complicit in censoring academic content.[16]

There is, of course, no easy solution here. As researchers and educators, we are tasked with not just exploring, analyzing, and seeking truth, we are also tasked with problematizing that very notion of what truth means. It is a difficult and fraught process, but it is one that we must endure. If in our increasing reliance on Chinese overseas students, we seek to exceptionalize these students to such an extent that we do not discuss certain topics, then we have a severe problem. However, if we limit our classrooms and our research collaboration only to those we agree with, we are guilty of another egregious form of censorship or indeed racism in our treatment of those we consider other. As researchers we have many ethical responsibilities, to our subject, to our students, and our collaborators and interlocuters, these ethical issues are not just theoretical, they are fraught with risk. There is a potential in the future that we will be required to only teach and research that which is not sensitive, the danger of this should be obvious to anyone concerned for education and the role of the university. All we can do is seek to find a balance whereby the presence of international students is seen for the positive it is while challenging those same students to reflect on the decolonializing of knowledge that has happened in their own countries. It is a fundamental ethical discussion, and ethics is essential to security in all cases.

Policy Recommendations

Recommendations for Academics

Do not self-censor on what might be considered sensitive topics. There has never been a greater need to challenge this silencing of discussion. Seek all

[15] Pringle and Woodman, "Between a Rock and a Hard Place: Academic Freedom in Globalising Chinese Universities," 1782–1802.

[16] Ibidem.

opportunities to engage in respectful discussion with Chinese academics, one in which all ideas are challenged and questioned in a constructive and supportive manner.

Recommendations for Universities

Do not allow the Chinese Communist Party to dictate what is taught or discussed in our universities for the sake of economics. Collaboration with Chinese academics and the presence of Chinese students in our universities greatly enriches us, but also, we should not view China as a source of income over true partnership.

Recommendations for Governments

It has never been more important to engage with Chinese academics, and governments should be very careful to avoid prejudice and paranoia when engaging with Chinese colleagues. However, it must also be realistic when it comes to organizations such as the Confucious Institutes which are branches of the Chinese government and which seek to influence how we discuss and research China.

Bibliography

Burawoy, Michael. "Decolonizing Canons: A Conversation with Chinese Sociologists." *In Interrogating the Future: Essays in Honour of David Fasenfest*. Brill, 2004.

Chen, Kuan-Hsing. *Asia as Method: Toward Deimperialization*. Duke University Press, 2010.

Chen, Stella. "Ideological and Political Education." *The China Media Project*, December 17, 2001, https://chinamediaproject.org/the_ccp_dictionary/ideological-and-political-education/.

Czymoniewicz-Klippel, Melina, Bianca Brijnath and Belina Crockett. "Ethics and the Promotion of Inclusiveness Within Qualitative Research: Case Examples From Asia and the Pacific." *Qualitative Inquiry* 16, no. 5, (2010): 332–341, DOI: 10.1177/1077800409358872.

Lin, Jin. "Rediscover Lasting Values: Confucian Cultural Learning Models in the Twenty-first Century." in *Re-envisioning Chinese Education: The Meaning of Person-making in a New Age*. Routledge, 2016.

Lin, Kequan. "Chinese Ideology in the Political Education of Students: How Does Ideology-Based Teaching Impact Students' Consciousness?" *Journal of Knowledge Economy* (2024), DOI. 10.1007/s13132-024-02164-9.

O'Brien, David and Melissa Shani Brown, *People, Place, Race and Nation in Xinjiang China: Territories of Identity*. Palgrave Macmillan, 2022.

Pratt, Bridgette, Cassandra Van, Cong Yali, Harun Rashid, Nandini Kumar, Aasim Ahmed, Ross Upshur and Bebe Loff. "Perspectives from South and East Asia on Clinical and Research Ethics: A Literature Review." *Journal of Empirical Research on Human Research Ethics* 9, no. 2 (2004): 52–67, DOI: 10.1525/jer.2014.9.2.52.

Pringle, Tim and Sophia Woodman. "Between a Rock and a Hard Place: Academic Freedom in Globalising Chinese Universities." *The International Journal of Human Rights* 26, no. 10 (2022): 1782–1802, DOI. 10.1080/13642987.2022.2074979.

Xu, Liu, Zhao Xiantong and Hugh Starkey. "Ideological and Political Education in Chinese Universities: Structures and Practices." *Asia Pacific Journal of Education* 43, no. 2 (2023): 596–598, DOI. 10.1080/02188791.2021.1960484.

Zeng, Jinghan. "Ideological and Political Education in China." In *The Chinese Communist Party's Capacity to Rule. Critical Studies of the Asia-Pacific*. Palgrave Macmillan, 2016.

https://doi org/10 59862/k7m2x9q4r8/16

Chapter 16

Internationalization, the Securitization of Knowledge, and Trans-National Repression within and beyond the Classroom

MELISSA SHANI BROWN
Jagiellonian University
ORCID: 0000-0002-2322-597X

Abstract: Trans-national repression, governments reaching beyond their borders to attempt to threaten and silence their citizens abroad, is a growing challenge within increasingly internationalized university environments. However, it remains a critically under-recognized threat. This report focuses on the ways TNR poses distinct challenges not only for research but also for teaching, and the need to recognize its role in the wider securitization of knowledge and the information wars. It uses the case study of the Chinese Communist Party (CCP) as an illustrative example, before turning to key recommendations for universities and governmental institutions.

Keywords: Trans-national repression (TNR), Chinese Communist Party (CCP), information wars

Introduction

The internationalization of universities presents diverse challenges for the securitization of knowledge. While there has been a wider turn of attention to the dangers to academia of the likes of data mining, academic/industrial espionage, cyber-attacks, and “post-truth”/”fake news,” the challenge of trans-national repression (TNR) regularly goes unmentioned. Yet it is a critical area in need of recognition and response. It is indelibly linked to “internationalization,” the increasing recruitment of staff and students from multiple origin countries, as well as the likes of foreign funding of research institutes or positions or scholarships. But it is also escalating due to the affordances digital technologies give to surveillance and trans-national communication. It is part of the wider "information wars," but carried out through forms of direct or indirect personal threat and violence. Universities are in fact extremely vulnerable to being sites of TNR and are in need of being part of the response to it. Turning a focus toward TNR highlights how much teaching—not only research—is in need of nuanced securitization.

Drawing on a variety of recent research, as well as more than ten years' personal experience teaching at universities in Europe, the United Kingdom, and China, I use a recurring focus on the Chinese Communist Party (CCP), not because they are unique, but are illustrative of some of the techniques and challenges.[1] I begin with defining and discussing TNR, before situating it in the wider securitization of knowledge, and finishing with a discussion of some of the recommendations given by others, focusing specifically on university responsibilities and responses.

Universities' Vulnerabilities to Trans-National Repression

Trans-national repression (henceforth TNR) is defined as:

> "[G]overnments reaching across borders to silence dissent among diasporas and exiles, including through assassinations, illegal deportations, abductions, digital threats, Interpol abuse, and family intimidation. … Transnational repression is no longer an exceptional tool, but a normal and institutionalized practice for dozens of countries that seek to control their citizens abroad."[2]

And while there has been longer-term research and attention to the experiences of the likes of exiled journalists or human rights activists as victims

[1] See: The Freedom House case studies: they identify that at least six countries are currently operating highly active campaigns of TNR, their cases being China, Russia, Iran, Saudi Arabia, Türkiye, Rwanda (”Freedom in the World,“ *Freedom House*, 2024).

[2] Yana Gorokhovskaia and Cathryn Grothe, "Freedom in the World 2024: The Mounting Damage of Flawed Elections and Armed Conflict," *Freedom House*, 2024. See also: "World Report 2024: Events of 2023," *Human Rights Watch*, 2024.

of TNR,[3] it has only more recently been identified that one of the most vulnerable groups are in fact international students.[4]

Indeed, universities are a *key site* of TNR[5] and it is precisely because they are spaces of communication that they are sensitive. They bring together students and staff—and others, we might consider guest speakers here—and, at least in places guaranteeing freedom of expression, encourage the discussion of diverse opinions and perspectives. But universities are inherently porous, all the more so as digital technologies mean that what is said or done is visible online.[6] One reason why there has been less attention to student experiences is that much of the TNR experienced by this group is far more "low-level" than the likes of assassination or abduction: nevertheless both human rights' groups and academics have increasingly pointed to the need to recognize the significance of surveillance, threat, and intimidation being carried out against students, staff, and others, at universities.[7]

The Case of the CCP

The CCP has long been criticized for curtailing both academic freedom and freedom of expression within China, particularly around sensitive or political issues—but it has also regularly attempted to impact upon academic and public debate beyond its borders.[8] It has appealed to other governments to

[3] Gerasimos Tsourapas, "Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics," *International Studies Review* 23, no. 3 (2021), https://doi.org/10.1093/isr/viaa061.

[4] "The State of the World's Human Rights: April 2024," *Amnesty International*, 2024. It is also worth noting that the likes of activists, or exiled journalists, regularly depend on student scholarships or research positions to leave their home countries, and thus such examples often also regularly fall within the broader university environment.

[5] Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue," in *Academics in a Century of Displacement*, edited by Leyla Dakhli, Pascale Laborier and Frank Wolff (Springer, 2024).

[6] Noura Al-Jizawi, Siena Anstis, Sharly Chan, Adam Sen, and Ronald J. Deibert, "Annotated Bibliography Digital Transnational Repression," *The Citizen Lab*, The University of Toronto. 2021. https://citizenlab.ca/wp-content/uploads/2021/05/Annotated-Bibliography-Digital-Transnational-Repression-May-2021.pdf.

[7] "The State of the World's Human Rights: April 2024," *Amnesty International*, 2024; "World Report 2024: Events of 2023," *Human Rights Watch*, 2024.

[8] Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue."

prevent speakers at academic conferences,[9] and numerous academics working on sensitive topics or who publicly criticize Chinese government policy have experienced forms of anonymous online intimidation or ambiguous threat from Chinese representatives. However, the CCP's systematic targeting of Chinese students has only more recently become a focus of attention. Some of this was an outgrowth of increased attention to specific cohorts of Chinese students—such as Uyghurs, Tibetans, or other ethnic minorities, as well as students from Hong Kong—who sought support from human rights groups and/or universities as they experienced increased surveillance due to political tension back home.[10] Yet the likes of Amnesty International reports identify a much wider policing of students beyond these groups.

Be they undergraduates, Masters, or PhD candidates, Chinese students must navigate a banal and pervasive context of a sense of surveillance and political sensitivity,[11] feeling judged for what classes they attend, what opinions they voice (or remain silent on) in class, what topics they choose to research, what search terms they put into personal computers, and even what conversations other students have on the likes of collective class WhatsApp groups. Posts on non-Chinese social media—such as Facebook, X, even encrypted apps such as Telegram—are also monitored. Many students self-censor what they say in class, but also what they include in assessments, under the impression that that may be monitored (e.g., via spyware on their computers), or held in accessible university repositories. Students who choose to actively engage with sensitive topics, or join student groups seen to do so, regularly experience forms of intimidation. But the awareness of the danger of being monitored and threatened is endemic across all Chinese students, an extension of the level of political control within China felt far beyond its borders.

[9] See, for example: "The Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China," *The China Tribunal*, 2020, 15. The PRC pressured the Israeli Ministry of Health via the Israeli Ministry of Foreign Affairs to prevent human rights lawyer David Matas from speaking at an international academic conference on the ethical challenges around human organ transplants in 2007, where China's organ transplant procedures were to be discussed.

[10] See: David Tobin and Nyrola Elimä, "'We Know You Better Than You Know Yourself': China's Transnational Repression of the Uyghur Diaspora," *University of Sheffield*, 2023.

[11] Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue."

Forms of intimidation vary. Many students are warned against expressing criticism of the CCP, or to discuss sensitive topics, told in vague terms that this may impact their careers, or that they are putting themselves in danger. It is clear that there is extensive digital surveillance,[12] tracking online communication, as well as forms of physical monitoring in host countries: students have been followed, photographed, or directly approached. In many cases, it is their family members back in China who receive direct threats—told that they may fail 'political background checks' necessary for employment or promotion or pensions because of what their children are studying or engaged in, in other cases family members have been detained by police. Students have been financially cut-off, sometimes willfully by their parents, or when parents are detained. In other cases, students themselves have been detained by the security services upon returning to China, for example for having a VPN.[13] In some cases, fellow classmates or friends, including non-Chinese students, also experience forms of intimidation, either anonymously online, or in some cases being followed on campuses or to their homes.[14]

A number of reports have identified that students experiencing this often receive little support from their universities, even though it is the university environment that partially creates the very circumstances they find themselves in.[15] This is partly because many universities have paid little attention to the growing phenomenon of TNR, and the way it impacts both students and staff. Amnesty International notes cases of non-Chinese university staff actively distancing themselves and not responding to politically active Chinese students or those experiencing TNR, "fearing the association might im-

[12] Noura Al-Jizawi, Siena Anstis, Sharly Chan, Adam Sen and Ronald J. Deibert, "Annotated Bibliography Digital Transnational Repression."

[13] Darren Byler, *Terror Capitalism: Uyghur Dispossession and Masculinity in a Chinese City* (Duke University Press, 2022).

[14] Amnesty International, *The State of the World's Human Rights: April 2024* (Amnesty International, 2024), 36.

[15] Tim Pringle and Sophia Woodman, "Between a Rock and a Hard Place: Academic Freedom in Globalising Chinese Universities," *The International Journal of Human Rights* 26, no. 10 (2022); Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue."

pair … access to research opportunities in China."[16] Such cases of disengagement are directly complicit with the isolation and marginalization that are integral to the types of threat deployed against such students. Universities have not only a duty of care towards their students (and staff), but they also need to see TNR as part of a broader threat to academic freedom and something they should increasingly be aware of and actively respond to.[17]

It is crucially important to differentiate different agents here. Other Chinese students sometimes play an active role, asserting pro-CCP opinions on- and offline, and at times arguing with or threatening Chinese students (or others) perceived to be critical. This can include confrontations with staff researching or teaching on China, particularly those actively criticizing the government or its narratives. Crucially: some of this must be respected as *genuine opinion* and thus their own freedom of expression, and when they are not receiving direction from state bodies they should not be considered state agents, although institutions may demand that they respect others' rights to freely express criticism.[18] This does however create a challenging environment when the relationship between the Chinese state, other organizations (such as the CSSA: the Chinese Scholar and Student Association, or Confucius Institutes), and Chinese citizens generally, can be difficult to disentangle, particularly when the state actively uses the latter.[19]

The Coercive Side to Information Wars

Some of this must be situated in the wider context of political tension and "information wars."[20] That is the reason why such practices of intimidation

[16] Amnesty International, https://www.amnesty.org/en/. See also: "The State of the World's Human Rights: April 2024," *Amnesty International*, (2024): 55.

[17] Fung Tsui and Shui Yu, "Activism in the Face of Repression: UK Universities as Allies for Hong Kong Activist Students and Academics," *UNESCO Chair, Protection of Human Rights Defenders and Expansion of Political Space*, 2023; "The State of the World's Human Rights: April 2024," *Amnesty International*, 2024; Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue."

[18] "The State of the World's Human Rights: April 2024," *Amnesty International*, (2024): 35.

[19] Kennedy C.-P. Wong, "Sowing Hate, Cultivating Loyalists: Mobilizing Repressive Nationalist Diasporas for Transnational Repression by the People's Republic of China Regime," *American Behavioral Scientist* 68, no. 12 (2024), https://doi.org/10.1177/00027642241267931.

[20] Vanessa Frangville, "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue."

are happening: this is an attempt to control what is communicated, how, and to whom. It is thus inextricable from wider discussions of academic freedom and human rights such as freedom of expression and association. It should also turn our attention toward the fact that "information wars" are already being fought within the academy.

Others have written about tackling "post-truth" or "disinformation" in educational settings such as through increased "critical literacy" or "inoculation against dis-information" curricula.[21] But it is crucially important to recognize that the problem of disinformation is not confined to "crazy conspiracy theorists" posting on YouTube. State actors, and expert bodies, are also actively disseminating disinformation.[22] The CCP disseminate factually inaccurate or contested information not only regarding contemporary issues (e.g., numbers of COVID-19 fatalities, BRI statistics, or more "sensitive" topics such as accusations of human rights abuses), but also across a range of other topics such as history.[23] These are disseminated via outlets as diverse as YouTube videos, news aggregation sites, academic mailing lists, as well as ostensibly neutral international organizations such as UNESCO.[24] The CCP is also actively manipulating search engine results on platforms such as Google and Bing, and through open-access academic publishing. Indeed, Vrije Universiteit in the Netherlands shut down a research center (Cross Cultural Human Rights Center (CCHRC)) funded by a Chinese university from Chongqing after it was revealed that academics associated with the center had been on trips to the Xinjiang region and appeared on state broadcasting denying there were any issues around discrimination for Uyghurs, or that "western" concepts of human rights were applicable to China.[25] But this example illustrates that the-

[21] Josh Compton et al., "Inoculation Theory in the Post-Truth Era: Extant Findings and New Frontiers for Contested Science, Misinformation, and Conspiracy Theories," *Social and Personality Psychology Compass* 15, no. 6 (2021).

[22] Vigjilenca Abazi, "The European Union Whistleblower Directive: A 'Game Changer' for Whistleblowing Protection?" *Industrial Law Journal* 49, no. 4 (2020).

[23] This must be recognized as geopolitical, since this is often linked to territorial claims in the present.

[24] Melissa Shani Brown and David O'Brien "The silk roads and shared heritage in Europe: Beyond 'China to Rome'" *China Information* 39, no. 3 (2025), DOI: 10.1177/0920203x241281989.

[25] Jon Henley, "Dutch university gives up Chinese funding due to impartiality concerns," *The Guardian*, January 25, 2022, https://www.theguardian.com/world/2022/jan/25/dutch-university-gives-up-chinese-funding-due-to-impartiality-concerns.

re are serious questions for academia regarding what counts as disinformation. Politically propagandistic narratives, spurious statistics, and obscured data are to be found in traditionally credible sources, such as peer-reviewed articles in ranked journals in mainstream publishers and reports from apparently credible research institutes. China is not unique. Russia is also engaging in similar techniques to sculpt public opinion beyond their borders, as are other states.[26] This means that both students and staff work in an environment where the credibility of information needs incessant questioning, where "truth" is highly politicized, and this will become more difficult to navigate with the increased use of AI making it harder to discern fakery.

TNR is a part of these wider issues, and should more ready be presented among them, as the use of fear, coercion, and force alongside more amorphous censorship or propaganda. Importantly, it highlights that there are high personal stakes involved in the content of university curricula and encouragement of freedom of expression within internationalized university settings. While this is certainly a significant challenge, universities need to recognize that they are not necessarily safe places for students or staff to engage in direct discussion of sensitive topics and turn to the question of how they may be made more so.

Recommendations

Although the crucial first step is the need to recognize that TNR affects the security of universities, it is worth turning to the question of what might be done in the face of this. Amnesty International offers a series of recommendations for national governments, international bodies (e.g., the EU), as well as academic institutions.[27] Recommendations for universities include the need to formulate explicit policies (e.g., explicitly establishing codes of conduct related to TNR), as well as procedures: mechanisms for reporting and supporting those experiencing it (e.g., anonymous reporting mechanisms, emergency financial aid, IT support for suspected cases of spyware,

[26] Gabriele Cosetino, Social Media and the Post-Truth World Order: *The Global Dynamics of Disinformation*, (Palgrave Macmillan, 2020).

[27] See full recommendations: "The State of the World's Human Rights: April 2024," *Amnesty International*, (2024), 55–58.

clear guidelines for reporting to local police, and seeking support from other agencies). Such recommendations should be considered, and universities should also broaden their understanding of whether or what forms of TNR their own communities (staff and students) may be experiencing—including through cross-university dialogue and practice sharing.

But in tackling TNR, universities and governments should recognize that it is a part of a many-pronged approach to controlling knowledge and communication by diverse states. And in light of this, forms of response need to connect it to other forms of securitizing knowledge within academies and research institutions. But a lesson from TNR is an important one: blanket suspicion of students (or staff) hailing from particular backgrounds cannot address these problems, because it is often people among their number who are most in need of protection and most vulnerable to having their families or futures threatened because of what they say or do. Any approaches must therefore recognize the fact that solidarity and sensitivity, not simply suspicion, must inform responses to the security challenges brought by internationalization.

Policy Recommendations

Recommendations for Scholars

More academic research is needed to document and explore the nuances of TNR. This includes:

- Generating more nuanced vocabularies to discuss the diversity of ways TNR operates both on- and offline and discussing different agents and forms of vulnerability and complicity (e.g.: people may simultaneously be "victims" and "perpetrators" of TNR, experiencing pressure and exerting it on others). Simplistic terms, such as blanket approaches, cannot but fail to address this complex issue justly.
- Researching experiences of TNR: across different university contexts (i.e., in different countries beyond the UK/USA which have hitherto been the main focus), across different national groups, comparing experiences between different groups within university contexts (e.g., staff, students, undergraduate vs. postgraduate, etc.), researching roles

of wider diaspora groups both in offering support to those experiencing TNR but also at times being complicit with it, as well as exploring different responses being put into practice by universities, and perceptions of their effectiveness or shortcomings.

Recommendations for Universities

There needs to be wider recognition that TNR is affecting university communities. Forms of response should include:

- The formulation of clear policies that cover TNR. These could be in the form of Codes of Conduct, focusing on the respect for academic freedom, integrating other forms of academic ethics (e.g., misconduct), applied across the student body. Such an approach would avoid targeting specific groups of students based on nationality and provide a flexible framework.
- The establishment of procedures to respond to allegations and to support those experiencing TNR.
- Awareness raising among both staff and students.

Recommendations for Government Institutions

There needs to be wider awareness of TNR and how it affects universities and university communities within educational ministries in order to support cross-institutional policies and procedures.

Government institutions already dealing with TNR (e.g., police, immigration etc.) should work in concert with educational institutions and relevant ministries in order to tailor responses.

***

Please note that the Amnesty International report "On my Campus, I am Afraid" (2024) offers extensive recommendations to universities, governments, and other institutions.

Bibliography

Abazi, Vigjilenca. "Truth Distancing? Whistleblowing as Remedy to Censorship during COVID-19". *Industrial Law Journal* 49, no. 4 (2020), doi:10.1017/err.2020.49.

Al-Jizawi, Noura, Siena Anstis, Sharly Chan, Adam Sen, Ronald J. Deibert. "Annotated Bibliography Digital Transnational Repression." *The Citizen Lab*, 2021. https://citizenlab.ca/wp-content/uploads/2021/05/Annotated-Bibliography-Digital-Transnational-Repression-May-2021.pdf.

Amnesty International. "'On my campus, I am afraid': China's targeting of overseas students stifles rights." *Amnesty International*, May 13, 2024. https://www.amnesty.org/en/documents/asa17/8006/2024/en/.

Amnesty International. "China: Overseas students face harassment and surveillance in campaign of transnational repression." *Amnesty International*. May 13, 2024. https://www.amnesty.org/en/latest/news/2024/05/china-overseas-students-face-harassment-and-surveillance-in-campaign-of-transnational-repression/.

Brown, Melissa Shani and David O'Brien. "The silk roads and shared heritage in Europe: Beyond 'China to Rome.'" *China Information* 39, no. 3 (2025), DOI: 10.1177/0920203x241281989.

Byler, Darren. *Terror Capitalism: Uyghur Dispossession and Masculinity in a Chinese City*. Duke University Press, 2022.

"The Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China: Judgement". *The China Tribunal*, March 1, 2020. https://chinatribunal.com/final-judgment-report/chinatribunal_judgment_1st-march_2020/.

Compton, Josh, Sander van der Linden, John Cook and Melisa. "Inoculation theory in the post-truth era: Extant findings and new frontiers for contested science, misinformation, and conspiracy theories." *Social Personal Psychology Compass*, May 5, 2021. https://doi.org/10.1111/spc3.12602.

Cosetino, Gabriele. *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation*. Palgrave Macmillan, 2020.

Frangville, Vanessa. "Constraints on Academic Freedom in the People's Republic of China: A Transnational Issue." In *Academics in a Century of Displacement*, edited by Leyla Dakhli, Pascale Laborier and Frank Wolff. Springer. 2024.

"Transnational Repression". *Freedom House*. 2024. https://freedomhouse.org/report/transnational-repression.

Henley, Jon. "Dutch university gives up Chinese funding due to impartiality concerns." *The Guardian*. January 25, 2022. https://www.theguardian.com/world/2022/jan/25/dutch-university-gives-up-chinese-funding-due-to-impartiality-concerns.

"Q&A: Transnational Repression". *Human Rights Watch*. June 12, 2024. https://www.hrw.org/news/2024/06/12/qa-transnational-repression.

Pringle, Tim and Sophia Woodman. "Between a Rock and a Hard Place: Academic Freedom in Globalising Chinese Universities." *The International Journal of Human Rights*. 2022. doi:10.1080/13642987.2022.2074979.

Tobin, David and Nyrola Elimä. "We know you better than you know yourself": China's transnational repression of the Uyghur diaspora." *The University of Sheffield*. https://www.sheffield.ac.uk/media/42149/download?attachment.

Tsourapas, Gerasimos. "Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics." *International Studies Review* 23, no. 3 (2021). https://doi.org/10.1093/isr/viaa061.

Tsui, Fung and Shui Yu. "Activism in the Face of Repression: UK Universities as Allies for Hong Kong Activist Students and Academics." *UNESCO Chair, Protection of Human Rights Defenders and Expansion of Political Space*, 2023.

Wong, Kennedy C.-P. "Sowing Hate, Cultivating Loyalists: Mobilizing Repressive Nationalist Diasporas for Transnational Repression by the People's Republic of China Regime". *American Behavioral Scientist* 68, no. 12 (2024). https://doi.org/10.1177/00027642241267931.

Authors' biographies

Izabela Albrycht is a Director of the Cybersecurity Centre and FORT Kraków DIANA Accelerator Poland Site Lead at AGH University of Kraków, the Rector's Proxy for NATO DIANA, an active member of Cyber LEGION, national cybersecurity programme led by the Cyberspace Defence Component Command (DKWOC) of the Polish Ministry of National Defence. She brings many years of experience serving in expert groups of Polish and international public institutions as well as business organisations, including the Council for Digitization at the Ministry of Digital Affairs (2016–2025), the Security and Defence Council under the National Development Council (2021–2025), DIGITAL EUROPE (2020–2022), and the Global Future Council on Cybersecurity at the World Economic Forum (2019–2022). In 2020–2022, she represented Poland in the NATO Advisory Group on Emerging and Disruptive Technologies, where she co-created the concept of NATO's DARPA, later named DIANA (Defence Accelerator for the North Atlantic). She is as a member of the Supervisory Board of Asseco Data Systems S.A. and ComCERT S.A. Previously, she served as Chair of the Kosciuszko Institute (2010–2021), one of Poland's leading think tanks, where she co-founded the European Cybersecurity Forum – CYBERSEC, a major cybersecurity conference in Central and Eastern Europe. She is a political scientist, a graduate of the Jagiellonian University in Kraków.

David O'Brien, Ph.D. is Marie Skłodowska-Curie Fellow at the Centre for International Studies and Development, Jagiellonian University, in Krakow, Poland. He was formerly at Ruhr University Bochum in Germany, and before that was based at the Chinese campus of Nottingham University. His work explores ethnic identity and ethnic policy in the People's Republic of China and Taiwan. His research has appeared in China Quarterly, International Politics, Journal of Current Chinese Affairs, and Asian Ethnicity, among others. He is co-author with Melissa Shani Brown of People, Place, Race, and Nation in Xinjiang, China: Territories of Identity (Palgrave Macmillan, 2022). He is also a frequent contributor to international media and has appeared in Financial Times, Reuters, Washington Post, AP, Deutsch Welle, Irish Times, RTE Radio and Television (Irish national broadcaster), Globe and Mail, among others.

Melissa Shani Brown, Ph.D. is an Ulam NAWA Visiting Fellow at the Centre for International Studies and Development, Jagiellonian University in Krakow, Poland. She was previously affiliated with Ruhr University Bochum in Germany, and before that she was based at the University of Nottingham's China campus, where she was an Assistant Professor in Media and Cultural Studies in the School of International Communications. Interdisciplinary in both research interests and training, her work explores the commodification of cultural heritage in tourism, the conceptualization of identities, and ethnic cultures in China (specifically in the Xinjiang region). Her research has appeared in China Quarterly, Journal of Current Chinese Affairs, Asian Ethnicity, Continuum, and Culture, Theory and Critique, among others.

Marek Czajkowski, Ph.D. is a political sciences professor at the Jagiellonian University in Krakow. Currently, the main field of his interest is space security, investigated from the point of view of political sciences, particularly international security. His most recent articles can be found online: Anti-Satellite Weapons: A Political Dimension (2021), Sino-American Rivalry in Space—Selected Strategic and Political Issues (2021), Anti-Satellite Weapons—Current Status (2024), Russo-Ukrainian War's Impact on Space Security: the Western Perspective (2024), and Space-Based Systems and Counterspace Warfare—a chapter in Routledge Handbook of the Future Warfare (2025).

Andrii Davydiuk, Ph.D. holds a PhD in Cybersecurity and is a Plans and Coordination branch head at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). He serves as Deputy Branch Head at the State Cyber Protection Centre under the State Service of Special Communications and Information Protection of Ukraine. Additionally, he is a senior research scientist at the G.E. Pukhov Institute for Modelling in Energy Engineering at National Academy of Sciences of Ukraine.

Leo Eigner is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich. His areas of research include knowledge/research security, science diplomacy, and Swiss and international science and technology policy more broadly. He holds a MPhil in Modern European History from the University of Oxford and a BA in History from King's College London. Before joining the CSS in 2023, he worked at the Swiss Science Council, the advisory board to the Federal Council for all issues related to science, education, research, and innovation policy.

Pawel Frankowski Ph.D. is Associate Professor of National Security at the Faculty of International and Political Studies at Jagiellonian University in Krakow. His research areas include international theory, international security, technology and international trade. He is principal investigator for the Polish National Science Centre project entitled "Labour standards in free trade agreements and preferential trading agreements of the European Union," and is currently completing a book on the nexus of politics, labor rights, and international trade regimes. He also works on a project on the role of diplomacy and space relations at the end of the Cold War, funded by the European University Institute and European Space Agency. He has published four books, two co-edited volumes, and multiple articles and chapters on space security, technology trade, and perspectives in international relations.

Marcin Grabowski, Ph.D. is an Associate Professor at the Institute of Political Science and International Relations of the Jagiellonian University of Krakow. He has been the founding Director of the Centre for International Studies and Development (2019-2025). Marcin graduated in International Relations from the Jagiellonian University in Krakow. He studied at Columbia University in the City of New York (School of International and Public Affairs), George Washington University in Washington (Sigur Center for Asian Studies), and University of California, San Diego, where he completed the Global Leadership Institute program. Marcin's research interests focus on the Asia-Pacific Rim, especially institutional arrangements of the region (APEC, ASEM, ASEAN, EAS, ARF, SAARC), American and Chinese foreign policies, theories of IR, with the special focus on complexity theory, and the International Economics. He has actively engaged in i.e. the following international scholarly associations: International Studies Association, Global International Relations Section (ISA-GIRS), Central and Eastern European Studies Association (CEEISA), European Association for Development Research and Training Institutes (EADI) holding leadership positions there.

Artur Gruszczak is a Professor of Social Sciences, Chair of National Security at the Faculty of International and Political Studies, Jagiellonian University in

Krakow. His principal interests and research areas include: intelligence studies; European intelligence cooperation; transformation of war and the future of warfare. Recently he co-edited with Monika Sawicka and Aleksandra Zdeb Democracy and its Fragility (Routledge 2026).

Marcin Jerzewski is the Head of the Taiwan Office of the European Values Center for Security Policy. He also serves as an analyst contributing to the Center's research on Taiwan and the broader Indo-Pacific region. Concurrently, he is also a Fellow with Visegrad Insight and an individual member of the Expert Pool at the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE). His previous professional experience includes work at the Taiwan NextGen Foundation, the Taipei City Government, the Polish Office in Taipei, and the Woodrow Wilson International Center for Scholars in Washington, DC. A sinologist and political scientist, Jerzewski completed his studies at National Chengchi University, University of Richmond, and University of Michigan-Ann Arbor.

Aleksi Kajander, LL.M, is a law researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). He is also a PhD candidate and Early Stage Researcher at the Tallinn University of Technology for Law and Technology. He holds a Master's degree in Investment Treaty Arbitration from Uppsala University as well as a Master's degree in Law and Technology from the Tallinn University of Technology.

Eliza Kotowska is a Risk Intelligence Analyst at TE Connectivity, where she analyzes geopolitical developments and global risk trends to support business risk mitigation. Previously, she served as a Project Coordinator and Analyst at the Kościuszko Institute (Instytut Kościuszki), a leading Polish think tank focused on cybersecurity, disinformation, and geopolitical security. In that role, she contributed to initiatives aimed at strengthening cybersecurity resilience, including the CYBERSEC European Cybersecurity Forum. She holds a Bachelor's degree in Criminology and Forensic Psychology from John Jay College of Criminal Justice and a Master's degree in International Security and Development from Jagiellonian University. Her work bridges academic research and applied risk analysis to help safeguard people and business operations.

Piotr Kwiatkowski, Ph.D. graduated in both Oriental Studies and Middle and

Far East Studies from the Jagiellonian University in Krakow and then prepared his PhD dissertation in the Oriental School of the University of Warsaw, then continued his studies at Renmin University in Beijing and Shida University in Taibei, recently a research assistant in POLONEZ BIS-2 programme entitled 'Narrating the 'new silk road': Chinese 'huayuquan' (discourse power) in OBOR/BRI externally-directed propaganda' led by Dr David O'Brien.

Filip Borges Månsson was the Executive Assistant (EA) at the Institute for Security & Development Policy (ISDP) and is currently studying a Master of arts (MA) degree in Military History at the Swedish Defence University. Mr. Borges Månsson holds a Bachelor of Arts (BA) in Political Science with a minor in History from Stockholm University and is a former exchange student at the University of Warsaw where he focused on Security and Foreign Policy Studies. Additionally, Mr. Borges Månsson has studied Intelligence Operations and Threat & Risk Management at the Swedish Defence University throughout his tenure at ISDP as EA. His areas of interest include international security policy issues, military history, European-Asian relations, geopolitics, intelligence, and risk management.

Marcin Przychodniak is a senior research fellow and China analyst in the Asia -Pacific program at the Polish Institute of International Affairs. His research mainly focuses on China's foreign policy and internal affairs. In 2012, he received a doctoral degree in the field of political science from Warsaw University. In 2005, he graduated from Adam Mickiewicz`s University (MA in political science with two faculties: foreign affairs and journalism). Between 2012 and 2016, he worked as a diplomat in the political section at the Embassy of the Republic of Poland in Beijing.

Błażej Sajduk PhD, is a political scientist and assistant professor at the Department of National Security of the Jagiellonian University and deputy head of the Center for Quantitative Research on Policy. He is a participant of numerous management and business courses (e.g., Zeppelin Universität, Ivey Business School) and training devoted to military aspects of the use of modern technologies (e.g., conducted by the Joint Special Operations University). He is an expert collaborator of Nowa Konfederacja, and a security and education expert at the Analysis Center of the Jagiellonian Club. His research interests include the ethical and social dimensions of the use of the latest technologies (especially AI and 5G), and political analysis. He is the author of a monograph and several dozen studies, scientific and popular science articles in the field of the role of new technologies for modern security and international relations.

Niklas Swanström, Ph.D. is the Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) and a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI). His main areas of expertise are conflict prevention, conflict management, and regional cooperation; Supply chain security, cyber warfare, and disinformation; Chinese foreign policy and security in Northeast Asia; the Belt and Road Initiative, traditional and non-traditional security threats, and its effect on regional and national security, as well as negotiations. Dr. Swanström holds a Ph.D. in Peace and Conflict Studies from Uppsala University.

Vladimir Sazonov, Ph.D. is Associate Professor at the University of Tartu and Research-Professor at the Estonian Military Academy. He holds a PhD in History from the University of Tartu (2010) and a PhD in Cultural Studies from the University of Tallinn (2020). He teaches courses on the politics, history, and security of the Middle East and Russia, and supervises BA, MA, and PhD theses. Vladimir Sazonov was recently the principal investigator of the research project "Russia's historical and political narratives in the Kremlin's influence activities targeting Western (including Estonian) and Ukrainian audiences in context of the Russo-Ukrainian war" (University of Tartu), and is currently the principal investigator of the research project "The strategic partnership between Russia and China and the use of artificial intelligence in information influence operations 2025–2027" (Estonian Military Academy/University of Tartu/Tallinn University of Technology).

Sławomir Wyciślak, Ph.D. is an Associate Professor at the Institute of Economics, Finance and Management, Jagiellonian University in Krakow, Poland. He specializes in risk management, business continuity, digital platforms, and systemic approach in management. Dr. Wyciślak has extensive experience in international research projects and has published articles on risk management and digital platforms. Dr. Wyciślak's work bridges the gap between theoretical frameworks and practical applications in the field of risk management and digital platforms in academic settings.

THE REPORT: RESEARCH AND EDUCATION SECURITY ILLUSTRATES CHALLENGES CONNECTED WITH THE PECULIARITY OF SECURITIZATION OF THE ACADEMIA, AS WELL AS RESEARCH PROCESS AND RESULTS. ON THE ONE HAND, OPENNESS TO THE GLOBAL RESEARCH AND STUDY COMMUNITY IS A CRUCIAL FEATURE OF THE ACADEMIA AND RESEARCH PROGRESS, BUT ON THE OTHER IT BRINGS ADDITIONAL RISK TO THE PROCESS AND A NECESSITY TO SAFEGUARD IT, ESPECIALLY IN THE CONTEXT OF GEOPOLITICAL RISKS CAUSED BY ACTORS LIKE RUSSIA OR CHINA. UNDERSTANDING THAT ACADEMIA CANNOT BE ISOLATED FROM EXTERNAL INFLUENCES, AS IT BENEFITS A LOT FROM OPENNESS TO THE WORLD, RESEARCHERS, STUDENTS AND R&D SECTORS MANAGERS SHOULD BE AWARE WHAT KIND OF RISKS 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, BRINGING OFTEN INVENTIONS AND PROVIDING PROGRESS.