Occasional Analysis Brief Series

KONRAD ADENAUER STIFTUNG
REGIONAL PROGRAMME AUSTRALIA AND THE PACIFIC

PERISCOPE

Analysis #18 January 2024

Research institutions between the poles of freedom of research and scientific espionage

Mag. Daniela Kirchmeir MA

While the danger of industrial espionage in companies is widely known and information security is recognized as a necessary measure, the phenomenon of espionage in the field of science was hardly addressed until a few years ago. In those cases where it was addressed, it was understood in terms of research competition: the researcher who was able to publish research findings first was seen as their author — regardless of whether they had obtained the findings illegitimately.

In recent years, however, the topic of scientific espionage has been more widely discussed (especially in the USA and Australia) and it has been recognized that espionage is not only carried out by individual researchers to accelerate their careers, but also on behalf of the state.

However, the discourse on this topic is confronted with three major problems: scientific espionage is challenging to grasp conceptually, hard to detect, and often operates in a legal gray area. Questions arise about what constitutes legitimate sharing of research results, what might be potentially illegitimate but not illegal information acquisition, and how this relates to espionage on behalf of a foreign state.[1] These unresolved issues lead to a low awareness of risks and a high undisclosed number of incidents.

In a time of global power struggles, it is not surprising that powerful nations aim to strengthen their position in the global political system. In the competition for dominance, nations also resort to scientific espionage, aiming to capture innovations, undermine sanctions and export controls, and shift the financial risks of research and development onto others. China is not the only actor using scientific espionage for these purposes, but it currently leads in terms of the efforts to obtain and the scope of collected data.[2] Even Russia and North Korea, known for comprehensive espionage activities,

1 Roper (2014), p. 9.
2 Roper (2014), xii, 18.

currently do not concentrate resources on espionage as targeted as China does.[3] China's scientific espionage activities can be closely linked to its strategic ambition to become the new world power by its 100th anniversary.

In most cases, scientific espionage is focused on dual-use research areas. In science, "dual use" refers to civilian research with a dual, namely military, purpose. In some fields of research, the dual-use-aspect is obvious, such as biochemistry, which is beneficial to human health but can also be used for chemical warfare agents. Or think of rocket technology, which enables us to explore space but can also be used for weapons. Dual-Use also includes areas that appear "neutral" at first glance, such as findings from materials research, nanotechnology, robotics, quantum technology and many more.[4] These potentially affected research areas are regulated by export controls in most countries. However, the types of control regimes use are not sufficient to counter the dangers posed by scientific espionage. The decision on whether something falls into the dual-use category or not remains dependent on the assessment within research institutions.[5] The responsibility for assessing the risks of research in a dual-use context is often delegated to individual researchers, who find themselves in an unresolved conflict: protecting sensitive research results while adhering to the ideal of research freedom,[6] and facing individual motivations, such as promoting international collaboration for prestige, financial incentives, or better career opportunities.[7]

Measures to protect research results are often considered contradictory to research freedom. However, the ideal of a free knowledge market has little evidence when closely examined. Research freedom is constrained by cultural practices, institutional regulations, and external pressures.[8]

It is obvious that the freedom of research is also influenced by the funding bodies (such as industry), which determine what research is carried out through their funding. The fragility of the ideal of research freedom is evident in scientific collaborations between Western countries and China. Two fundamentally different political and cultural systems with partly antagonistic value systems collide. While Western countries like Germany and Australia emphasize democracy, the rule of law, and the principle of research freedom, the scientific sector in autocratic China is closely intertwined with the state and the Communist Party.[9] This is reflected in the hierarchical organization of leadership bodies at Chinese universities, where — unlike in Western countries — the party chief ranks higher in the hierarchy than the academic leader. This ensures that the research institution aligns with the party's agenda.[10]

The strategy paper of the Communist Party known as "Document No. 9", which was leaked in 2013, revealed that universal Western values such as freedom, democracy, and human rights are vehemently rejected by the CCP. This attitude also affects the Academic Freedom Index of the country, with China ranking among the worst ten percent in 2023 (see figure 1).[11]

3 Idwisch-Drentrup (12.03.2020).
4 Deutsche Forschungsgemeinschaft e.V./Deutsche Akademie der Naturforscher Leopoldina e.V. (2014), p. 9
5 Joske (2018), p. 18.
6 The term "research freedom" means that scientists can decide for themselves what topics they research and what methods they use. This principle also gives scientists and researchers the freedom to share their knowledge and publish their results
7 Eckert u. a. (18.05.2022a).
8 Sismondo (2010), p. 190ff.
9 F itzgerald (2017), p. 8.
10 Hamilton (2018), p. 115.
11 Friedrich-Alexander-Universität Erlangen-Nürnberg/V-Dem Institute (2023), p. 3.

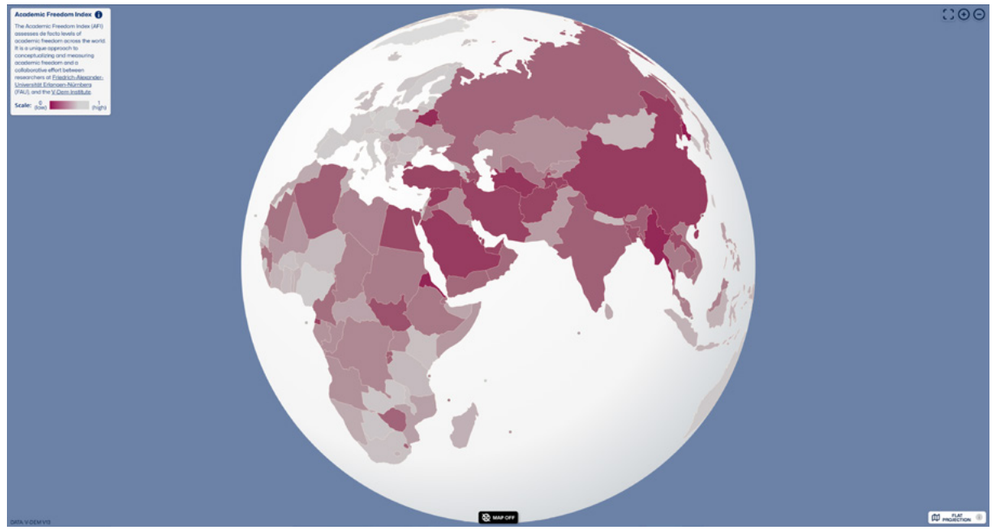

Figure 1: Academic Freedom Index Map[12]

The need for financial resources compels research institutions to look for financially potent partners. This can undermine research freedom, as evident in Europe and Australia, especially considering that foreign investments inherently carry the potential for "foreign influence."[13] In the West, awareness of foreign influence, particularly with a focus on China, is growing and is sometimes even referred to as a central societal challenge of the 21st century. Simultaneously, there is a warning not to let the discussion devolve into xenophobia.[14]

Regardless of whether one speaks of "foreign influence" or "scientific espionage", research institutions and universities are often easy targets. The lack of awareness among individuals, the uncertainty about what knowledge is worth protecting, and the absence of a holistic security concept for protecting research results facilitate the work of so-called "non-traditional collectors"[15] — students and visiting scholars from China who gather information deemed relevant by the People's Republic during their professional activities.[16]

Herein lies the dilemma, a tension between progress and security. Consequently, international research collaboration is also referred to as a double-edged sword: it is indispensable to keep a nation at the forefront of time, but it can also become a gateway for espionage.[17] Scientific espionage not only leads to unfair competition, job losses, and weakening national security but can also have geopolitical consequences if one thinks of the military build-up in China and the current conflict between the People's Republic and Taiwan. Moreover, research institutions affected by espionage face reputation damage and the loss of trust from society and sponsors. [18] This dilemma needs resolution.

12 https://academic-freedom-index.net (25.01.2024)
13 The term "foreign interference" refers to covert, deceptive or corrupt activities that originate from a foreign state actor and undermine the sovereignty of the state concerned or run counter to its values and interests. (Directorate-General for Research and Innovation (2022), p. 7; Australian Government (02.01.2024).
14 Mansted (Feb 2021), p. 3, 17.
15 Non-traditional collectors are individuals whose primary profession is not intelligence collection but who gather sensitive information on behalf of government entities. (Federal Bureau of Investigation (2019), p. 1.).
16 Boyd u. a. (September 2010), p. 44.
17 Zenglein/Holzmann (2019), p. 12f.
18 Eftimiades (2020), p. 36 f.

In the 2022-initiated study “Research institutions between the poles of freedom of research and protection of knowledge. Scientific espionage using the example of China”,[19] the question was examined of how research institutions can protect themselves from scientific espionage. Using expert interviews, the study investigated how research institutions in Austria overcome the tension between protection against scientific espionage and the necessity of scientific exchange. The interviewees included individuals from the research sector, as well as experts from security authorities and intelligence services. Through qualitative research methodology, an inventory was generated, and recommendations were derived.

Similar to Sabine Carl’s findings for Germany in 2019, awareness of scientific espionage in research institutions in Austria was very low. Since risk awareness is a prerequisite for all subsequent measures, sensitization should occur at the following levels:

- Politics: The political commitment to knowledge protection forms the foundation, as it is a prerequisite for adequate resource allocation and the representation of the phenomenon in legislation.
- Authorities: The empirical study revealed that certain reservations exist among research institutions towards intelligence and security agencies. This is associated with an increase in the number of unreported suspicions. Therefore, authorities should actively work to reduce inhibitions.
- Research institutions: At both leadership and employee levels, there is often a prevailing understanding that protective measures hinder innovation in research. Striking a balance between enabling innovation and safeguarding knowledge from illegitimate access or misuse is essentially a risk management process. Only when university leaders and researchers recognize that risk management considers opportunities as well as risks can a productive approach to knowledge protection be ensured. Workshops and training sessions raise awareness of the dangers of scientific espionage.

The next step is the establishment of knowledge protection at the institutional level. To do this, a target analysis must be conducted regularly, identifying which research areas of an organization need protection. Only when precise knowledge is available about which scientific topics of the institution might be targeted for espionage can targeted measures be implemented. This includes identifying the “crown jewels”, which are the most sensitive or valuable research results. The result of the target analysis is reflected in cross-institutional protective measures, including monitoring and vetting processes. This means that scientific collaboration is assessed in terms of its potential risks, which can be derived from the research goal, the orientation of the partner university, and the background of the foreign researcher. In order to identify threats and espionage potential, it is also necessary to look at the interests of other nations. Since it is hardly reasonable to expect researchers or research organizations to inform themselves about the national interests of partner countries in addition to their scientific work, security authorities and intelligence services should provide support here. However, it must be clear where the limits of their areas of competence are in order to avoid giving the impression of censorship: While the security authorities and intelligence services can pass on their expertise regarding threats and espionage methods to the research institutions, the latter must be able to remain autonomous in deciding which fields of research are sensitive. Individual researchers cannot be required to identify and assess the risks of their own research, as this would place them in a conflict of interest. Internal legal and ethics department expertise should be involved in this evaluation.

The implementation of an information security management system is a technical measure for securing research results. This includes ensuring basic IT security, sandboxing, using multi-factor authentication,

19 Kirchmeir (2023).

and introducing access and entry restrictions. To counter the prejudice that such security measures inhibit creativity, it may be helpful to introduce an innovation management process, for example, based on the Stage-Gate process by Cooper.[20] A process-oriented approach ensures finding synergies, quality assurance, and information security. Research projects are divided into individual, sequentially structured project phases with different security levels. While openness is significant in the initial phase to stimulate exchange between researchers and foster innovation, the need-to-know principle restricts access to information towards the end to prevent endangering the exploitation of results.

The majority of individuals interviewed in the empirical study shared the assessment that scientific espionage will increase in the future. Therefore, a clear strategy for dealing with this risk is needed. In the course of upcoming research projects, particular attention should be paid to emphasizing practical relevance. How research institutions can develop appropriate protective measures, tailored to their size, orientation, and available resources, should be investigated. The result of these efforts should be a modular knowledge protection concept that is standardized but can be adapted to the needs of stakeholders and aims at synchronizing the efforts of individual stakeholders.

20 Cooper (1990), p.46.

About the Author

Mag. Daniela Kirchmeir MA

Daniela Kirchmeir works as an Information Security Consultant at HiSolutions (Berlin). After completing her degree in education in 2018, she worked in the education sector for four years. In 2023, she completed her master's degree in integrated risk management at the University of Applied Sciences Campus Vienna. In her research on scientific espionage, she dealt with the difficult balancing act between freedom of research and knowledge protection and identified prevention methods for the sustainable protection of research results. 2023 she was awarded first place in the Security category at the European Students Research Conference for her master's thesis.

Bibliography

Australian Government (Hg.) (2024): Department of Home Affairs Website. URL: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference (02.01.2024).

Boyd, Dallas/Lewis, Jeffrey G./Pollack, Joshua H. (September 2010): Advanced technology acquisition strategies of the People's Republic of China.

Cooper, Robert G. (1990): New products: The key factors in success.

Deutsche Forschungsgemeinschaft e.V./Deutsche Akademie der Naturforscher Le-opoldina e.V. (2014): Wissenschaftsfreiheit und Wissenschaftsverantwortung. Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung.

Directorate-General for Research and Innovation (2022): Tackling R&I foreign inter-ference. Staff working document, Luxembourg.

Eckert, Till u. a. (18.05.2022): Chinesisches Militär made in Germany. Wie Deutschland China hilft, zur Militär-Supermacht aufzusteigen, in: correctiv. URL: https://correctiv.org/aktuelles/wirtschaft/2022/05/18/wie-deutschlands-wissenschaft-china-hilft-zur-militaer-supermacht-aufzusteigen/ (18.5.2022).

Eftimiades, Nicholas (2020): A series on chinese espionage. Operations and tactics, [Etats-Unis].

Federal Bureau of Investigation (2019): Case Example: Non-traditional collectors, URL: https://www.fbi.gov/file-repository/china-case-example-insulation-2019.pdf (04.12.2022).

Feldwisch-Drentrup, Hinnerk (12.03.2020): Spionage durch China: Deutschlands gefährliche Naivität, in: WELT. URL: https://www.welt.de/politik/deutschland/plus206504433/Spionage-durch-China-Deutschlands-gefaehrliche-Naivitaet.html (12.3.2020).

Fitzgerald, John (2017): Academic Freedom and the Comteporary University. Lessons from China. In: Humanities Australia Journal, S. 8–20. URL: https://www.humanities.org.au/wp-content/uploads/2017/09/AAH-Academy-Lect-Fitzgerald-2016.pdf (02.01.2024).

Friedrich-Alexander-Universität Erlangen-Nürnberg; V-Dem Institute (Hg.) (2023): Academic Freedom Index. Update 2023. URL: https://academic-freedom-index.net/research/Academic_Freedom_Index_Update.pdf (25.01.2024).

Friedrich-Alexander-Universität Erlangen-Nürnberg; V-Dem Institute (Hg.) (2023): Academic Freedom Index (AFI). URL: https://academic-freedom-index.net/ (02.01.2024).

Hamilton, Clive/Ohlberg, Mareike (2021): Die lautlose Eroberung. Wie China west-liche Demokratien unterwandert und die Welt neu ordnet., 6. Aufl., München.

Joske, Alex (2018): Picking flowers, making honey, URL: https://www.aspi.org.au/report/picking-flowers-making-honey (07.06.2022).

Kirchmeir, Daniela (2023): Forschungseinrichtungen im Spannungsfeld zwischen Forschungsfreiheit und Wissensschutz. Wissenschaftsspionage am Beispiel China. URL: https://pub.fh-campuswien.ac.at/obvfcwhsacc/content/titleinfo/8865231 (25.01.2024)

Mansted, Katherine (2021): The Domestic Security Grey Zone. Navigating the Space Between Foreign Influence and Foreign Interference. Canberra: National Security College.

Roper, Carl (2014): Trade secret theft, industrial espionage, and the China threat. Boca Raton.

Sismondo, Sergio (2010): An introduction to science and technology studies. 2nd ed. Chichester, West Sussex, U.K., Malden, MA: Wiley-Blackwell.

Zenglein, Max J./Holzmann, Anna (2019): Evolving made in China 2025. China's industrial policy in the quest for global tech leadership., in: MERICS Papers on China, Nr. 8.

About the Periscope Series

'Periscope' is the Occasional Analysis Paper/Brief series of the Konrad Adenauer Foundation's Regional Programme Australia and the Pacific. Just like the real-world sighting instrument, Periscope is meant as a lens to broaden our insights - taking in views from different angles. This way, it seeks to bring together perspectives from Germany, Europe, Australia, New Zealand and the Pacific region to augment our understanding of contemporary issues and help address the pressing problems of our time. The Periscope Series covers topics from the area of foreign and security policy, cybersecurity, terrorism/counter-terrorism, energy policy, rule of law, socio-economic matters and development policy. It comprises both **longer Analysis Papers** – in the form of single-author (and co-authored) contributions or edited volumes with multiple authors - and **shorter Analysis Briefs**.

KONRAD ADENAUER STIFTUNG
REGIONAL PROGRAMME AUSTRALIA AND THE PACIFIC

Konrad Adenauer Stiftung (Australia) Ltd
Regional Programme Australia and the Pacific
www.kas.de/australia
periscopekasaustralia.com.au

Periscope – Occasional Analysis Brief Series #18 (January 2024).
ISSN: 2652-7332 (Online)