Freedom of research & protection of knowledge.

Scientific espionage using the example of China

Mag. Daniela Kirchmeir, MA

I. Introduction

While the danger of economic espionage is already anchored in the collective consciousness, **scientific espionage is still hardly addressed**. Scientific espionage is carried out by **foreign secret or intelligence services** and pursues **economic, scientific or political interests** (Carl, 2019).

There is a wide range of methods in scientific espionage: from cyberattacks to stealing research results and prototypes, taking photos, to social engineering and phishing emails. Since many fields of research fall into the **dual-use area**, critical voices are now growing louder calling for stronger safeguards in this area (Hannas & Chang , 2021).

Since several years **China** in particular has been coming into focus as a player in the field of scientific espionage because of its **aggressive information-gathering strategy**. By tapping into foreign knowledge, China circum-vents **financial risks and expands its supremacy** (Joske, 2018).

Research institutions are an easy target for espionage because of the following reasons:

1. Most of them have neither developed a **holistic security concept** nor precisely deter-mined which of their knowledge is worth protecting.
2. It's difficult to put a **monetary figure** on the damage caused by scientific espionage.
3. **International cooperations** (which are often a gateway for scientific espionage) are seen as key figures in the scientific field. Concerns about cooperation with foreign research institutions are usually rejected with reference to freedom of research (Carl, 2019).

II. Research Question

Existing reports and studies do not allow a direct assessment of the situation regarding espionage at Austrian research institutions. Therefore, no statement can be made about:

- How domestic research institutions are **affected** by scientific espionage.
- The degree of **risk awareness** in the research institutions.
- What **measures** the research organisations take to protect their knowledge and how **effective** they are.

Therefore, the research question is: **How can Austrian research institutions protect their knowledge against scientific espionage?**

III. Methods

The empirical study (October 2022 - March 2023) focused on the analysis of a selected sample using a **qualitative research methodology**. 12 semi-structured interviews with experts from the following fields were conducted:

- **research institutions**
- **security agencies**
- **intelligence services**
- **experts from other institutions with special expertise**

The (co-)generated data was evaluated and interpreted on the basis of **qualitative content analysis** (Kuckartz, 2018).

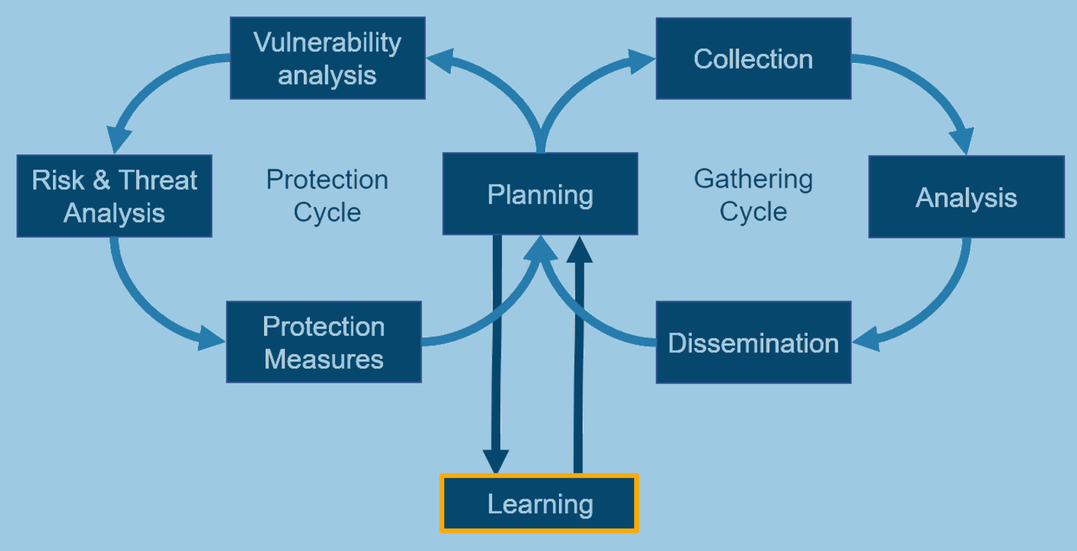
IV. Results

The empirical study showed: The **balancing act between enabling freedom of research and protecting knowledge** from illegitimate access is essentially a **risk management process**. Measures are needed on the following levels:

1. **Government**
   a) Cooperation between the ministries should be intensified in order to derive measures from the needs identified by these actors from their respective expert perspectives and to jointly develop a **knowledge protection concept** for research institutions.
2. **Security agencies & intelligence services**
   a) Security agencies and intelligence services should present their areas of **competence** and communicate them more clearly.
   b) Cooperation between security agencies, intelligence services and research insti-tutions should be **institutionalized** in order to identify **mutual interests and needs**.
   c) The clear naming of **contact persons** in the respective organizations would reduce inhibition thresholds, strengthen trust and increase the willingness to report.
3. **Research institutions**
   a) Research institutions should make use of **awareness training** provided by the Austrian intelligence services to raise awareness of scientific espionage within their own ranks.
   b) They should subject research collaborations to ongoing **monitoring**, assess for threats, and establish **vetting processes**.
   c) Research institutions should carry out a **target analysis** to determine what know-ledge they should protect. From this they should derive **specific measures**.

V. Discussion & Conclusion

For the implementation of knowledge protection, an orientation towards Brouard's and Sprott's **Intelligence Gathering & Protection Cycle** is recommended, since the acquisition and protection of information are **two sides of the same coin** (Brouard & Sprott, 2004). The cycle presents the responsibilities on both sides: The Protection Cycle can be used as orientation for the **research institutions**, the Gathering Cycle by the **security authorities**.



Given the initial situation in Austria this research project can only serve as a first stocktaking. Future research should involve the security authorities and intelligence services to **break down the barriers** between them and scientific organisations, eliminate blind spots and thus improve knowledge protection. **Best practices on knowledge protection** should be shared at **national** and **European level** in order to use resources efficiently.

Contact information

FH Campus Wien
University of Applied Sciences
Department of Integrated Risk Management
Favoritenstraße 226
1100 Vienna
Austria
risikomanagement@fh-campuswien.ac.at

References

Brouard, F. & Sprott, E. (2004). Business Intelligence for Canadian Corporations after September 11. *Journal of Competitive Intelligence and Management*, *2*(1), 1–15. https://carleton.ca/profbrouard/wp-content/uploads/2004ArticleJCIMBusinessIntelligence911Brouardfinal.pdf
Carl, S. (2019). Wissenschaftsspionage - Risiken für den deutschen Forschungsstandort? In E. Wallwaey, E. Bollhöfer & S. Knickmeier (Hrsg.), *Wirtschaftsspionage und Konkurrenzausspähung. Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern* (S. 137–167). Duncker & Humboldt.
Hannas, W. & Chang, H. (2021). Chinese Technology Transfer. An Introduction. In W. Hannas & D. Tatlow (Eds.), *China's Quest for Foreign Technology. Beyond Espionage* (pp. 3–20). Routledge Taylor & Francis Group.
Joske, A. (2018). *Picking flowers, making honey. The Chinese military's collaboration with foreign universities*. The Australian Strategic Policy Institute https://www.aspi.org.au/report/picking-flowers-making-honey

Master thesis (in German)

SCAN ME

Kirchmeir, D. (2023). *Forschungs-einrichtungen im Spannungsfeld zwischen Forschungsfreiheit und Wissensschutz. Wissenschafts-spionage am Beispiel China.* FH Campus Wien. https://pub.fh-campuswien.ac.at/obvfcwhsacc/content/titleinfo/8865231