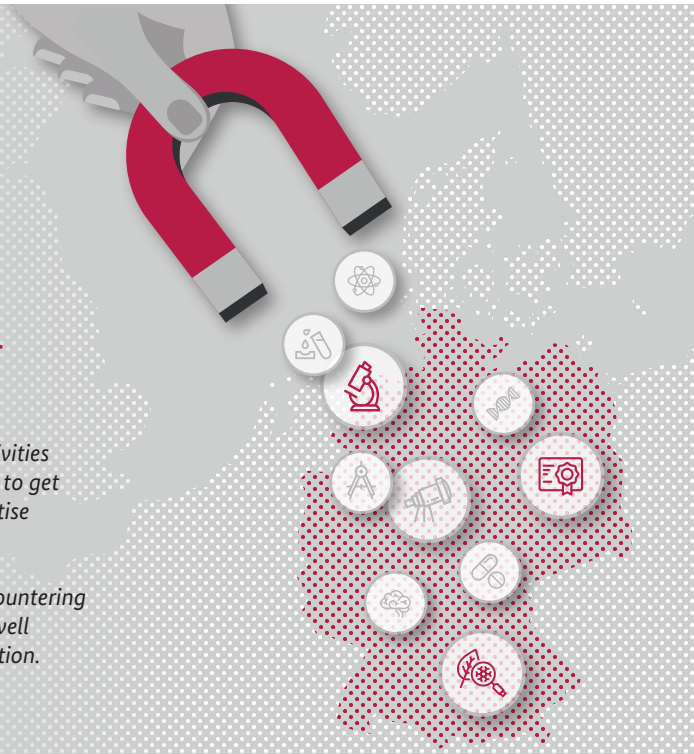
Info Blatt

Information sheets on economic security

Espionage in Science and Research



Universities and research institutions in Germany are the target of espionage activities emanating from foreign intelligence services. Those services use various methods to get access to information and expertise. The risk of an uncontrolled outflow of expertise can be minimised by implementing and respecting adequate security standards.

BfV and the domestic intelligence services of the federal states are in charge of countering espionage and sabotage activities carried out by foreign intelligence services as well as of countering extremism and will be at your disposal for confidential consultation.

Objectives and Implications of Scientific Espionage

- The primary **aim of scientific espionage** on behalf of foreign states is **to acquire information** in order to **be a step ahead in terms of knowledge** or to fill existing gaps in knowledge.
- State-sponsored attackers have **extensive personnel and financial resources** and operate systematically, skilfully and on a long-term basis.
- They meet with a scientific scene which tends to pay **insufficient attention** to ***security aspects*** and the risk posed by espionage.

- ***Security***
  Adherence to basic safety precautions will make the unintended outflow of expertise difficult.
  - *The expertise and know-how to be protected and related protection requirements have been defined.*
  - *The level of protection meets protection requirements.*
  - *There is a comprehensive security concept in place.*

RISKS

Scientific espionage may have considerable negative implications for the institution:

- *loss of orders, patents and profit*
- *cancellation of joint scientific projects*
- *loss of confidence and damage to image*

Scientific espionage is also, in the long term, a threat to Germany as an economic and scientific player.

RESEARCH AREAS AT PARTICULAR RISK

Certain countries have defined sectors in which they want to achieve a **leading role on the world market and/or more independence**. The expertise required to that end is obtained **by means of both legal and illegal methods**. Various **research fields** are a special focus of interest.

- Naval architecture and ocean engineering
- Energy saving and electromobility
- Information and communication technologies
- Automation and robotics
- Electricity plants
- Aerospace equipment
- New materials
- Agriculture
- Modern rail transport systems
- Biomedicine and high-performance medical equipment

Scientific Espionage: Modi Operandi and Precautions

In order to gather information, foreign intelligence services use different methods or a combination of them. Scientific institutions need a comprehensive safety concept to protect themselves, which covers the following aspects.

Foreign students / Guest scientists

BACKGROUND

- Foreign intelligence services also make use of **guest students and guest scientists** to gain access to research results.
- Nationals of their country are **placed under the obligation to collaborate**, are **pressurized or** are **offered baits**. Cooperation may also be **completely voluntary** for patriotic reasons.
- Sometimes existing **state affiliations** are deliberately **concealed** from the guest institution.

Example: *A guest scientist, specialist field: control engineering, engaged in research at a German university. What he concealed from the university: In his home country, he is the head of a military laboratory for rocket testing.*

SAFETY PRECAUTIONS

- When selecting scientific staff, please conduct background checks. Pay special attention to any connections to military institutions.
- Conclude non-disclosure agreements with staff members.
- Keep an eye on the guest scientists' careers even after they have left the institution.

Please also note our flyers "Methods of Espionage: HUMINT", "PreEmployment Screening" and "Insider Threats", which can be accessed via ***www.verfassungsschutz.de*** *(Service > Publications).*

EXCURSUS: CHINA

China wants to become the top nation in the fields of economy, science and military until 2049. At the same time, it is seeking to gain increasing economic independence from foreign countries.

- To achieve these aims, China also needs extensive Western knowledge. It uses both legal and illegal means to obtain such information.
- Long-term strategies and programmes contribute to attaining these objectives, for example by increasingly interlinking trade & industry, academic institutions and military (SEVEN SONS OF NATIONAL DEFENCE).
- Joint research projects on an international level and stays of scientists abroad are systematically promoted to bring special knowledge into the country. Of special significance are research results that may also be used for ***dual-use goods*** (e.g. materials research).

SEVEN SONS OF NATIONAL DEFENCE

- *The "Seven Sons" are universities that are particularly close to the military in research and teaching. But also other scientific institutions and research centres are known to have connections to the military sector. The database* ***China Defence Universities Tracker*** *may be consulted for a risk assessment in case of scientific cooperation projects.*
  - ***https://unitracker.aspi.org.au***

- ***Dual-use goods***
  Dual-use goods are products and goods that may be used for both civil applications and military purposes. Due to their risk potential, the export of these goods to countries outside Europe is subject to certain controls and restrictions.

Scientific Espionage: Modi Operandi and Precautions

Financing / Joint projects

BACKGROUND

- **Joint research projects and externally financed projects** may be exploited by foreign actors to acquire relevant knowledge. Research results may be used in their home country for **economic and military purposes**.
- In this connection, dual-use goods and/or ***knowledge of proliferation concern*** have an important role.

Example: *A German university is engaged in research, together with a foreign research institute, on a subject of materials science. The foreign university is known to be close to the military and the research results may find application for ultramodern weapon systems.*

Knowledge of proliferation concern

Knowledge of proliferation concern is expertise which is required to develop technologies for weapons of mass destruction and delivery systems. Scientific findings often have both civil and military applications. Being aware of this problem is a prerequisite to protecting information of proliferation concern..

SAFETY PRECAUTIONS

- **Evaluate the potential** of technologies and thoroughly assess the **research implications**.
- Examine potential cooperation partners as to whether there are any **connections to state bodies** and check the joint research project for any **possibilities of abuse**.
- **Make and document agreements** on the use of research data and results.

Cyber attacks

BACKGROUND

- Universities and other research institutions may become the target of state-controlled cyber attacks which are aimed at capturing sensitive research data.

Example: *By means of a phishing email, students are directed to the imitated registration page of the university library. The attackers can use the captured access data to penetrate into the computer network.*

SAFETY PRECAUTIONS

- Implement a cyber security strategy as part of a **comprehensive safety concept**.

Data/Processes

- *identify and classify sensitive information*
- *limit and regularly check rights of access to drives and data*
- *establish contingency plans, guidelines and checklists*
- *monitor data flows to detect any suspicious behaviour*
- *protect access by using strong passwords*

Hardware and software

- *use current operating systems and programmes*
- *close security gaps and install the newest updates*
- *make backups and keep them separately*
- *insert network security tools (IDS/IPS)*
- *protect emails through transport or end-to-end encryption*

Employees

- *raise the awareness of your employees for them to follow general safety precautions*
- *conduct training on specific subjects (data security, social engineering, phishing etc.)*
- *practise behaviour in the event of a crisis*
- *establish confidential reporting channels for the employees*

Approaches

BACKGROUND

- Foreign intelligence services try, by using various methods, to make **scientific experts**, for example when the latter travel abroad, **cooperate** with them to thus get direct access to sensitive research data.

Example: *A scientist is approached on a visit abroad by an alleged colleague, who asks her to provide an expert statement and offers payment in return. Subsequently, increasing interest in the actual research results becomes obvious. gezeigt.*

SAFETY PRECAUTIONS

- **Scientific staff** should be trained with regard to possible approaches by foreign intelligence services.
- Please ensure that **behaviour rules** for stays abroad do **exist and are made known**.

→ *Flyers: "Business Travel Security", "Methods of Espionage: HUMINT"*

Guest visits

BACKGROUND

- Members of foreign delegations might try to **elicit information from you, to evade security arrangements** or to **illicitly smuggle in electronic devices**.

Example: *Five additional foreign delegation members show up uninvited for a guided tour offered by a research department. During the guided tour, they repeatedly go away from the group without being authorised to do so, sometimes taking photographs of the facility.*

SAFETY PRECAUTIONS

- Formulate binding rules on how to deal with **technical devices** and **uninvited visitors**.
- Please ensure that all members of the visiting group have **a clearance** and that, if advisable, **a background check** was made.
- As for **sensitive areas**, please think about whether a visit is really necessary there.
- Please check in advance whether the route of the guided tour holds **visible sensitive information** (bulletin boards, monitors etc).
- Keep the group together and take care that **behaviour rules are observed**.

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

BfV (Bundesamt für Verfassungsschutz) and the 16 domestic intelligence services of the federal states are the domestic intelligence community. They cooperate closely in the field of preventive economic security. Thus a strong network is formed that extends to where your company is based. Please visit ***www.verfassungsschutz.de*** *to find a list of contacts at the federal state authorities.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

The Economic Security Initiative (Initiative Wirtschafts-schutz) is an initiative by BfV, BKA, BND and BSI. On their information platform ***www.wirtschaftsschutz.info*** *they offer their expertise in the field of economic security together with various partners. This includes the issue of cyber crime as well as economic and scientific espionage or IT security.*

Your direct contact to economic security

Ministerium des Innern und für Sport Rheinland-Pfalz
Wirtschaftsschutz
Schillerplatz 3-5
55116 Mainz
Tel.: 06131/16-3773
Email: wirtschaftsschutz@mdi.rlp.de