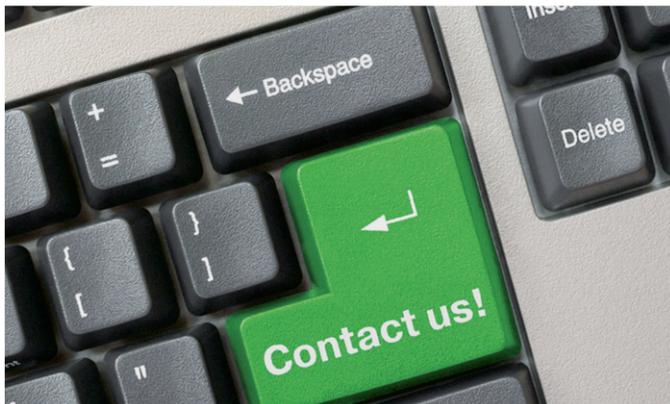


## Recommended action

- Designate a point of contact for security-related issues and communicate this within your organisation
- Check the sensitivity of your projects, test installations, results and the related documentation at an early stage
- Adapt the organisational, technical and personnel-related protective measures adequately
- Particularly when employing guest scientists, pay attention to our guidelines concerning staff selection (\*)
- Raise your employees' and students' awareness – especially in the run-up to stays and contacts abroad.

**Do not hesitate to contact us and make an appointment for confidential awareness talks**



\* cf. leaflet "Staff selection"

## Your points of contact in economic security



Protecting values in a concerted effort

For additional information and your local contacts' communication data, please visit the website.



[www.wirtschaftsschutz.info](http://www.wirtschaftsschutz.info)

### Imprint

Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © Gernot Krautberger - Fotolia.com  
© ccvision  
© Minerva Studio - Fotolia.com  
© Nikolai Sorokin - Fotolia.com

DOI: March 2016

## Domestic intelligence service



Federal Republic of Germany  
Federal States

## Economic Security

## Threats to Research and Teaching

## Threat potential

Innovations of German universities and research institutes characterise the German scientific landscape worldwide. Besides, they are a key pillar for the German economy's international success. Therefore, they are a coveted target of espionage for competitors and intelligence services of foreign states.



**Today's science will be tomorrow's economy**

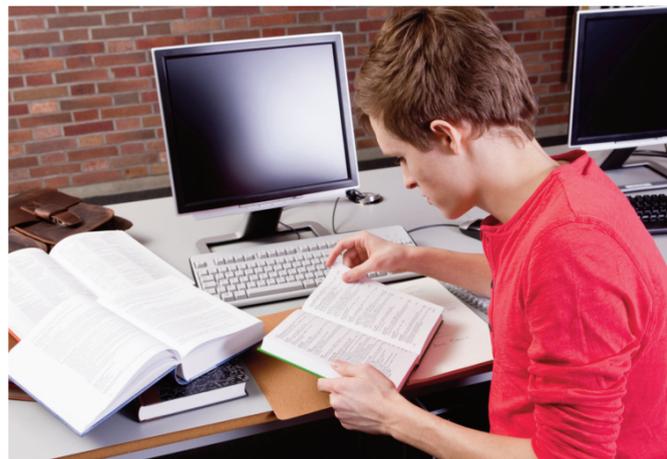
**Today's student will be tomorrow's decision-maker**

## Threat scenarios

Preliminary Social Engineering (\*) often forms the basis for attacks such as:

- spying on staff members of German universities and research institutes
- intelligence-related contact established with German students and scientists abroad
- electronic attacks on the internal network or integrated grid system of scientific institutes
- infiltration of guest students and guest scientists into promising research projects in Germany

The sending country can attach studies abroad/scholarships – provided to its students and scientists – to their willingness to carry out espionage activities. This obligation to support one's own country is often regarded as an honour.



\* cf. leaflet "Social Engineering"

## Further risks

The need to publicise results as widely and promptly as possible in the framework of the freedom of research and teaching is contrary to the requirement of the protection of know-how – a fact that should be taken into account in **scientific competition**.



**Development co-operations** can be used to unlawfully appropriate the partner's superiority in know-how.

**Projects funded by third parties** require special protection because also the sponsor's know-how and market position are affected. In the worst case, not only current but also future projects will be jeopardised.

If cases of an uncontrolled leakage of know-how become public, the research institute's or university's **reputation** may be at stake too.