



# **Forschungsspionage – und wie Sie sich schützen können**

## **Liebe Wissenschaftlerinnen und Wissenschaftler der Universität Bielefeld,**

zur Forschung gehören Offenheit, Vernetzung und grenzüberschreitender Austausch. Aufgrund der großen Chancen und Potenziale einer internationalen Zusammenarbeit ist die weitere Internationalisierung ein erklärtes Strategieziel der Universität Bielefeld. Doch im Zusammenwirken mit der Digitalisierung der Wissenschaft birgt die internationale Zusammenarbeit für eine Universität wie unsere, die in mehreren Forschungsfeldern weltweit zu den Spitzenstandorten zählt, auch Risiken: Die hier erbrachten Forschungs- und Innovationsleistungen stellen einen wichtigen Wettbewerbsfaktor dar, und nicht alle Wettbewerber halten sich an faire Regeln. Die Universität Bielefeld kann, wie auch andere Hochschulen, Ziel von Ausforschung zum Beispiel durch Wettbewerber oder Nachrichtendienste fremder Staaten werden. Auf diese Risiken wollen wir aufmerksam machen und gleichzeitig erste Handlungsempfehlungen aussprechen.

### **Digitalisierung**

Die Digitalisierung von Informationen und Kommunikationsmedien erzeugt Angriffspunkte für Ausforschungsaktivitäten.

So häufen sich Berichte über das Ausforschen mittels sog. Social Engineering. Dabei treten Angreifer beispielsweise über Fake-Profilen in den sozialen Netzwerken (z.B. LinkedIn, ResearchGate) mit Wissenschaftlerinnen und Wissenschaftlern in Kontakt und bauen behutsam eine persönliche Beziehung auf, um an Informationen zu gelangen. Daneben werden Hacking-Angriffe auf Forschungsprojekte beobachtet – oft über zielgerichtet präparierte E-Mails mit Schadsoftware im

Anhang. Auch Forschungsdaten auf Laptops oder mobilen Datenträgern führen auf Reisen zu einem Risiko, da sie entwendet oder bei Grenzübertritten ausgeforscht werden können.

Sie begegnen den Risiken, indem Sie sich klarmachen, welche Informationen in Ihrem Bereich schützenswert sind, und adäquate Abwehrmaßnahmen ergreifen. Wir unterstützen Sie gerne dabei. Ansprechpersonen finden Sie am Ende dieses Textes. Seien Sie aufmerksam bei Kontaktaufnahmen über soziale Netzwerke und teilen Sie dort keine vertraulichen Informationen. Bedenken Sie auch, dass die Weitergabe solcher Informationen Ihre wissenschaftliche Reputation und die Ihrer Einrichtung gefährden kann und dass Sie sich schlimmstenfalls strafbar machen. Führen Sie auf Reisen nur unbedingt notwendige Daten mit. Informieren Sie sich über Ein- und Ausfuhrbestimmungen in Ihrem Zielland und treffen Sie entsprechende Schutzmaßnahmen. Mitunter werden IT-Geräte an der Grenze beschlagnahmt, durchsucht und die Informationen kopiert.

### **Forschende Gäste**

Jedes Jahr kommen ca. 300 Wissenschaftlerinnen und Wissenschaftler aus der ganzen Welt für längere Aufenthalte nach Bielefeld. Dieser bereichernde Austausch kann auch Risiken mit sich bringen, die nicht sofort ersichtlich sind.

Es werden vermehrt Fälle dokumentiert, in denen Gaststudierende und Gastwissenschaftlerinnen und -wissenschaftler in Projekte eingeschleust werden, um diese auszuforschen und die Erkenntnisse an Dienste ihres Heimatlandes weiterzuleiten.



Wir raten Professorinnen und Professoren sowie den Leitungen von Arbeitsgruppen daher, bereits bei der Auswahl forschender Gäste zweifelhafte Initiativbewerbungen zu beachten und ungewöhnliche Verhaltensweisen oder auffällige Neugier zu hinterfragen. Machen Sie sich Gedanken über den Schutz Ihres wertvollen Know-hows. In Drittmittelprojekten kann bei Verlust oder Offenlegung von Forschungsergebnissen die Marktposition des Geldgebers betroffen sein und eine weitere Förderung auf dem Spiel stehen.

### **Forschungsaufenthalte im Ausland**

Im Rahmen zahlreicher Mobilitätsangebote der Universität Bielefeld reisen regelmäßig Bielefelder Wissenschaftlerinnen und Wissenschaftler für Forschungsaufenthalte ins Ausland.

Gerade Studierende und Universitäts-Mitarbeitende, die eine Karriere in Politik, Diplomatie oder (Energie- und Finanz-)Wirtschaft anstreben, sind für Geheimdienste ein interessantes Anwerbungsziel. Die Vorgehensweisen sind dabei vielfältig und reichen von der freundschaftlichen Kontaktaufnahme über die angebliche wissenschaftliche Förderung bis zu einer Druckausübung mittels vermeintlicher Gesetzesverstöße oder Ordnungswidrigkeiten bei der Einreise.

Informieren Sie sich im Vorfeld eines Auslandsaufenthaltes über Wissenschaftsspionage im Zielland, recherchieren Sie den Hintergrund von Personen, die mit Ihnen in Kontakt treten, und seien Sie besonders vorsichtig bei unerwarteten bzw. verdächtig erscheinenden Kontaktaufnahmen sowie bei der Weitergabe konkreter Informationen. Die Zusammenarbeit mit ausländischen Nachrichtendiensten stellt in Deutschland eine Straftat dar, und schon die Kontaktaufnahme kann Sie in eine unangenehme Situation bringen.

### **Bei Fragen wenden Sie sich an:**

#### **Michael Sundermeyer**

Informationssicherheitsbeauftragter /  
Information Security Officer (ISO)  
<https://www.uni-bielefeld.de/informationssicherheit>  
[informationssicherheit@uni-bielefeld.de](mailto:informationssicherheit@uni-bielefeld.de)  
Tel. 0521 106-3032

#### **Angelika Spilker**

Compliance-Beauftragte  
<https://www.uni-bielefeld.de.de/compliance>  
[compliance@uni-bielefeld.de](mailto:compliance@uni-bielefeld.de)  
Tel. 0521 106-3339

#### **Anna Balkenhol**

Compliance  
<https://www.uni-bielefeld.de.de/compliance>  
[compliance@uni-bielefeld.de](mailto:compliance@uni-bielefeld.de)  
Tel. 0521 106-3331



# Espionage in research an how to protect yourself

**Dear scientists of Bielefeld University,** research includes openness, networking and cross-border exchange. Due to the great opportunities and potential of international cooperation, further internationalization is a declared strategic goal of Bielefeld University. But in conjunction with the digitalization of science, international cooperation also entails risks for a university like ours, which is one of the world's leading research locations in several fields: The research and innovation achievements made here represent an important competitive factor, and not all competitors adhere to fair rules. Bielefeld University, like other universities, can become a target of research by competitors or intelligence services of foreign countries, for example. We want to draw attention to these risks and at the same time make initial recommendations for action.

## Digitalization

The digitization of information and communication media creates attack vectors for research activities.

Reports on research using so-called social engineering are accumulating. For example, attackers use fake profiles in social networks (e.g. LinkedIn, ResearchGate) to get in touch with scientists and cautiously establish a personal relationship in order to obtain information. Hacking attacks on research projects have also been observed - often via well prepared e-mails with malware attached. Research data on laptops or other mobile devices also pose a risk when traveling, as they can be stolen or investigated at border crossings.

You can mitigate the risks by making clear which information in your area is worth

protecting and by taking appropriate countermeasures. We will be happy to support you. Contact persons can be found at the end of this flyer. Be attentive when making contact via social networks and do not share any confidential information there. Also keep in mind that sharing such information can jeopardize your scientific reputation and that of your institution, and that in the worst case you could be prosecuted. Keep only essential information with you when you travel. Find out about import and export regulations in your destination country and take appropriate measures. Sometimes IT equipment is confiscated, searched, and copied at the border.

## Research guests

Every year about 300 scientists from all over the world come to Bielefeld for longer stays. This enriching exchange can also entail risks that are not immediately apparent.

More and more cases are being documented in which visiting students and scholars are introduced into projects in order to research them and pass on their findings to the services of their home country.

We therefore advise professors and heads of working groups to consider dubious unsolicited applications when selecting research guests and to question unusual behavior or conspicuous curiosity. Think about protecting your valuable know-how. In third-party funded projects, the loss or disclosure of research results may affect the market position of the donor and further funding may be at stake.



## Research stays abroad

Within the framework of numerous mobility Bielefeld University offers scientists from Bielefeld regularly travel abroad for re-search stays.

Especially students and university employees who are looking for a career in politics, diplomacy, energy or economics are an interesting recruitment target for secret services. The procedures are manifold and range from friendly contact to alleged scientific support to exerting pressure by means of alleged violations of the law or administrative offences on entry.

Find out about scientific espionage in the target country prior to your stay abroad, research the background of people who come into contact with you, and be particularly careful when making unexpected or suspicious contacts and when passing on concrete information. Cooperation with foreign intelligence services is a criminal offence in Germany, and even making contact can put you in an unpleasant situation.

## Feel free to contact us:

### Michael Sundermeyer

Informationssicherheitsbeauftragter /  
Information Security Officer (ISO)

<https://www.uni->

[bielefeld.de/informationssicherheit](https://www.uni-bielefeld.de/informationssicherheit)

[informationssicherheit@uni-bielefeld.de](mailto:informationssicherheit@uni-bielefeld.de)

Tel. 0521 106-3032

### Angelika Spilker

Compliance-Beauftragte

<https://www.uni-bielefeld.de.de/compliance>

[compliance@uni-bielefeld.de](mailto:compliance@uni-bielefeld.de)

Tel. 0521 106-3339

### Anna Balkenhol

Compliance

<https://www.uni-bielefeld.de.de/compliance>

[compliance@uni-bielefeld.de](mailto:compliance@uni-bielefeld.de)

Tel. 0521 106-3331