

## Antwort

der Landesregierung

auf die Kleine Anfrage Nr. 3089

der Abgeordneten Dr. Daniela Oeynhausen (AfD-Fraktion)

Drucksache 7/8475

### **Sicherheitsrelevante Forschung an Brandenburger Hochschulen**

Namens der Landesregierung beantwortet die Ministerin für Wissenschaft, Forschung und Kultur die Kleine Anfrage wie folgt:

Der Krieg in der Ukraine und auch mögliche Gefahren durch Wissensabfluss in die Volksrepublik China haben das Wesen des Politischen als Feld des Gegensatzes von Freund und Feind und damit auch die Notwendigkeit der Wahrung der eigenen Interessen gegen fremde Begehrlichkeiten wieder stärker ins Bewusstsein gerückt. Dies betrifft auch das Interesse Deutschlands und Brandenburgs, die eigene Forschung vor Missbrauch durch fremde Mächte, insbesondere deren Unternehmen oder Streitkräfte, zu schützen.

Ich frage die Landesregierung:

1. Gab es in den letzten zehn Jahren auf militärischem oder sonstigem sicherheitsrelevanten Gebiet eine Zusammenarbeit Brandenburger Forschungseinrichtungen mit Ländern außerhalb der NATO, die in den letzten zehn Jahren in einem kriegerischen Konflikt involviert sind/waren, mit Unternehmen aus diesen Ländern oder mit anderen Unternehmen, die oder deren Gesellschafter enge Beziehungen zu diesen Ländern pflegen? (Bitte die Projekte im Einzelnen anführen.)

Vorbemerkung: Zur Beantwortung der Fragen sind die staatlichen Hochschulen des Landes abgefragt und um Zuarbeit gebeten worden. Sofern sich die Fragestellung der Fragen 1 und 2 über den Wortlaut des Titels der KA hinausgehend auch auf außeruniversitäre Forschungseinrichtungen beziehen sollte, lautet die Antwort zu Frage 1 „Nein.“ und zu Frage 2 „Keine“.

Zur Frage 1: Keine der Hochschulen berichtet dabei von einer Zusammenarbeit auf militärischem oder sonstigem sicherheitsrelevanten Gebiet mit Ländern oder Unternehmen aus den in der Frage 1 genannten Gebieten.

Daten über die Zusammenarbeit der Hochschulen und Forschungseinrichtungen auf den in der Frage genannten Gebieten werden von der Landesregierung nicht erhoben. Erkenntnisse, die über die dargestellten Antworten der Einrichtungen hinausgehen, liegen der Landesregierung daher nicht vor.

2. Welche Fälle von schädlichem Wissensabfluss, insbesondere Spionage, gab es in den letzten zehn Jahren mit Bezug zu militärischer bzw. sicherheitsrelevanter bzw. Dual-Use-Forschung im Land Brandenburg? Personen mit welcher Staatsangehörigkeit, insbesondere nichtdeutscher Staatsangehörigkeit, waren darin verwickelt?

Zu Frage 2: Der Landesregierung sind keine derartigen Fälle bekannt.

3. Welche Sicherheitsmaßnahmen gibt es derzeit an den Brandenburger Hochschulen zum Schutz vor unerwünschtem Wissensabfluss ins Ausland, insbesondere vor Spionage? Welche Sicherheitsmaßnahmen und -konzepte haben die brandenburgischen Hochschulen bzw. Institute bzw. die Landesregierung seit Beginn des Ukrainekrieges wann entwickelt und umgesetzt? Bitte erläutern.

Zu Frage 3: Aus naheliegenden Gründen verbietet es sich, in einem öffentlichen Dokument konkret über einzelne Maßnahmen zu berichten.

Die Hochschulen verweisen zum Schutz vor unerwünschtem Wissensabfluss ins Ausland, insbesondere vor Spionage, auf die geltenden Regeln der Guten Wissenschaftlichen Praxis sowie projektbezogene Schutzmaßnahmen. Bei Forschungsvorhaben mit Auslandsbezug wird die Einhaltung der geltenden Außenwirtschaftsregelungen überprüft.

Ein Schwerpunkt der Sicherheitsmaßnahmen liegt im Bereich der IT-Sicherheit. So hat beispielsweise die TH Wildau seit 2017 ein Informationsmanagementsystem nach ISO 27001 zur allgemeinen Erhöhung der Informationssicherheit eingeführt, die TH Brandenburg hat ein Informationssicherheitsmanagementsystem eingeführt oder die Europa-Universität Viadrina ein Projekt zur Verbesserung der Datensicherheit initiiert. Weiterhin arbeiten alle Brandenburger Hochschulen über das Zentrum für digitale Transformation (ZDT) zusammen an Projekten Bereich Informationssicherheit. Im Zuge der 2021 abgeschlossenen Prüfung der IT-Sicherheit an den Brandenburger Hochschulen haben alle Hochschulen Maßnahmen ergriffen, die seinerzeit festgestellten Mängel abzustellen.

Maßnahmen der IT-Sicherheit sollen dabei grundsätzlich die Integrität, Vertraulichkeit und Verfügbarkeit der eigenen digitalen Ressourcen nachhaltig schützen und wirken somit regelmäßig nicht nur gegen eine spezifische Bedrohung. In diesem Rahmen wirken Verbesserungen der IT-Sicherheit aber auch dem Schutz vor Spionage.

Die Hochschulen setzen auch auf Sensibilisierungsmaßnahmen wie Fortbildungen oder Informationsveranstaltungen für die Mitglieder und Angehörigen der Hochschulen. Dabei werden Mitarbeitende und Forschende ausdrücklich auch für die Risiken von Wissensabfluss und Spionage sensibilisiert. Sie lernen, wie sie potenzielle Bedrohungen erkennen und abwehren können. Eine besondere Sensibilität besteht zudem bei Forschungsthemen mit Chi-nabezug.

4. Wie vielen Cyberangriffen waren die Brandenburger Hochschulen/Institute im Jahr 2022 aus welchen Ländern ausgesetzt, welche Zwischenfälle gab es in diesem Zusammenhang und welche Sicherheitsvorkehrungen haben die Hochschulen deswegen getroffen?

Zu Frage 4: Die Hochschulen sind täglich einer Vielzahl von Cyber-Angriffen unterschiedlichster Art und Intensität ausgesetzt, wobei ein Großteil dieser Angriffe nicht spezialisiert, automatisiert und durch Bots ausgeführt wird (z.B. Port- und Passwort-Scans). Niederschwellige Angriffsversuche werden kontinuierlich bzw. im Sekundentakt beobachtet. So berichtet beispielsweise die Universität Potsdam von täglich mehreren Tausend Denial-of-Service (DoS)- und Phishing-Angriffen. Die Angriffe werden nach Angaben der Universität überwiegend aus China, Korea, Russland, Ukraine, Niederlande, Pakistan, Brasilien, Rumänien und den USA abgesetzt. Die geographische Zuordnung der Angriffe ist jedoch nur bedingt aussagekräftig (hinzuweisen ist hier auf sog. False Flag Angriffe), da erfahrungsgemäß viele Angriffe von gekaperten Servern abgesetzt werden. Auch VPN- bzw. Proxy-Verschleierungstechniken können eine klare Lokation von Angriffen verhindern. Einige Hochschulen führen keine Erhebungen oder Analysen dazu durch, aus welchen Ländern Angriffe mutmaßlich stammen. Teilweise werden Anzahl und Herkunft diese Angriffe nicht protokolliert, da sie zur Standard-Gefährdungslage öffentlicher IT-Systeme zählen.

Die Viadrina berichtet für die vergangenen Jahre - neben dem konstant hohen Level an Phishing-Mails - drei Sicherheitsvorfälle: Im Mai und November 2022 jeweils ein DDOS-Angriff auf den Internetauftritt und Mitte Juni 2022 eine Ausnutzung einer Lücke in der VMWare-Umgebung, jedoch ohne Datenabfluss. Keines der Ereignisse war datenschutzrechtlich meldepflichtig.

An der HNEE gab es seit 2021/22 nur Sicherheitsvorfälle auf Grundlage von Phishing Angriffen, bei denen im Einzelfall Postfächer übernommen wurden. An der Fachhochschule Potsdam gab es 2022 zwei nicht näher spezifizierte Vorfälle. Die Filmuniversität Babelsberg berichtet für 2022 von keinen erfolgreichen gezielten Angriffen gegen die Hochschule.

Durch die von den Hochschulen ergriffenen technischen und organisatorischen Schutzmaßnahmen konnte bisher eine Beeinträchtigung der Verfügbarkeit, Vertraulichkeit und Integrität der IT-Infrastruktur in der Regel abgewendet werden. Jedoch sind im Einzelfall aufgrund von DoS-Attacken einzelne IT-Dienste zeitweise nicht erreichbar gewesen. Zudem wurden vereinzelt über gekaperte E-Mail-Accounts weitere SPAM- und Phishing-Mails abgesetzt.

Die Hochschulen haben in den letzten Jahren die Informationssicherheit durch zahlreiche Maßnahmen erhöht. Dazu zählen unter anderem der Ausbau von Firewalls, die Verbesserung der SPAM-Erkennung und die Etablierung von Prozessen für die Vorfallsbearbeitung. Zur zusätzlichen Sensibilisierung wurde zudem mit finanzieller Unterstützung des MWFK landesweit ein Awareness-Schulungstool ausgeschrieben, das an allen Hochschulen eingesetzt werden kann.

Im Übrigen wird zu den Sicherheitsmaßnahmen auf die Antwort zu Frage 3 verwiesen.