



## Schriftliche Anfrage

der Abgeordneten **Verena Osgyan, Florian Siekmann BÜNDNIS 90/DIE GRÜNEN**  
vom 25.03.2021

### Wirtschafts- und Wissenschaftsspionage durch China

Wir fragen die Staatsregierung:

- 1.1 Inwieweit sind der Staatsregierung Fälle bekannt, in denen Regierungen anderer Länder gezielt versucht haben, Daten aus der bayerischen Wirtschaft und Wissenschaft abzugreifen (Auflistung nach Datum, Vorfall, Schaden und Land)? ..... 3
- 1.2 Wie viele Fälle der Datenspionage sind insbesondere vor chinesischem Hintergrund bekannt (Auflistung nach Datum, Vorfall und Schaden)? ..... 3
- 1.3 Geht von China nach Ansicht der Staatsregierung eine besondere Gefahr in Bezug auf die illegale Informationsbeschaffung aus? ..... 3
  
- 2.1 Welche Maßnahmen ergreift die Staatsregierung, um Wissenschaftseinrichtungen und Unternehmen vor diesen Angriffen zu schützen? ..... 3
- 2.2 Inwieweit fördert die Staatsregierung Digitalisierungskompetenz, Datensicherheit und Cybersecurity, damit sich Unternehmen und Forschungseinrichtungen bestmöglich davor schützen können? ..... 3
- 2.3 Wie schätzt die Staatsregierung die Umsetzung einer Initiative wie in Baden-Württemberg ein, wo die Landesregierung den Hochschulen Informationssicherheitsbeauftragte zur Seite stellt? ..... 4
  
- 3.1 Inwieweit steht die Staatsregierung mit bayerischen Forschungseinrichtungen, Hochschulen sowie Unternehmen in Kontakt, um sich wegen potenzieller Cyberangriffe und Spionage auszutauschen? ..... 4
- 3.2 Welche Erkenntnisse liegen dem Landesamt für Sicherheit in der Informationstechnik im Hinblick auf Wissenschafts- und Wirtschaftsspionage aus China vor? ..... 4
- 3.3 Welche anderen staatlichen Stellen gibt es, um Forschung und Wirtschaft vor dem unbefugten Abgreifen von Informationen zu schützen? ..... 4
  
- 4.1 Welche Sicherheitsvorkehrungen spielen bei der Einstellung von chinesischen Wissenschaftlerinnen und Wissenschaftlern bei Forschungsprojekten und in Unternehmen eine Rolle? ..... 5
- 4.2 Welche Sicherheitsvorkehrungen erfolgen hier, damit sichergestellt wird, dass Informationen nicht an unbefugte Dritte weitergegeben werden? ..... 5
- 4.3 Wie viele Einrichtungen und Unternehmen haben den Beratungsdienst des Landesamtes für Verfassungsschutz („Wirtschaftsschutz“: Prävention durch Information) in den vergangenen Jahren in Anspruch genommen? ..... 5
  
- 5.1 Nachdem bekannt wurde, dass die chinesische Regierung hier lebende chinesische Staatsbürgerinnen und Staatsbürger gezielt zur Informationsbeschaffung aufsucht und anzuwerben versucht, welche Maßnahmen hat die Staatsregierung seitdem eingeleitet, um dies zu verhindern? ..... 5
- 5.2 Stehen hier lebende chinesische Staatsbürgerinnen und Staatsbürger diesbezüglich unter Beobachtung? ..... 5
- 5.3 Falls ja, wie viele Personen betrifft das? ..... 5

Hinweis des Landtagsamts: Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

6. Welche Erkenntnisse liegen der Staatsregierung darüber vor, dass die chinesische Regierung offenbar bewusst soziale Netzwerke nutzt, um Informantinnen und Informanten auch in Bayern anzuwerben? ..... 6
- 7.1 Inwieweit hat die Staatsregierung die chinesischen Nachrichtendienste, Ministry of State Security, Military Intelligence Department, Third Department, im Blick? ..... 6
- 7.2 Welche Aktivitäten chinesischer Nachrichtendienste (Ministry of State Security, Military Intelligence Department, Third Department etc.) im Freistaat sind der Staatsregierung bekannt? ..... 6
8. Sind der Staatsregierung Fälle bekannt, in denen weitere staatliche Einrichtungen (über den Wissenschaftsbereich hinaus) Ziel von Spionage sind oder waren? ..... 6

## Antwort

**des Staatsministeriums des Innern, für Sport und Integration im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat, dem Staatsministerium für Wirtschaft, Landesentwicklung und Energie, dem Staatsministerium für Wissenschaft und Kunst und dem Staatsministerium für Digitales**  
vom 24.04.2021

### Vorbemerkung:

Soweit Anfragen von Abgeordneten Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, ist zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (vgl. BVerfGE 124, 161 [189]). Nach sorgfältiger Abwägung des Informationsrechts der Abgeordneten mit dem Staatswohl, das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, ist das Staatsministerium des Innern, für Sport und Integration (StMI) zu der Auffassung gelangt, dass die Fragen 1.1 und 1.2 sowie der Fragenkomplex 5 der Schriftlichen Anfrage nicht beantwortet werden können. Auskünfte hierzu würden die Wirksamkeit der nachrichtendienstlichen Tätigkeit und auch die Sicherheitslage gefährden. Sie sind unter Spionageabwehraspekten besonders schutzwürdig.

Eine öffentliche Bekanntgabe detaillierter Informationen zu einzelnen Aufklärungsereignissen des Landesamtes für Verfassungsschutz (BayLfV) im Bereich der Spionageabwehr über die Aktivitäten von ausländischen Nachrichtendiensten und damit einhergehend die Kenntnisnahme durch Unbefugte hätte erhebliche nachteilige Auswirkungen auf die Sicherheit des Landes. Die preisgegebenen Informationen könnten insbesondere von ausländischen Nachrichtendiensten genutzt werden, um ihre Methoden und die eigene Erkenntnislage anzupassen. Die künftige Aufgabenerfüllung des BayLfV wäre somit erheblich beeinträchtigt. Hierdurch könnten signifikante Lücken mit Folgewirkungen für die Sicherheitslage im Freistaat Bayern und in der Bundesrepublik Deutschland entstehen.

Auch eine VS-Einstufung (VS = Verschlussache) und Hinterlegung der angefragten Informationen in der VS-Registrierung des Landtags würde ihrer erheblichen Relevanz im Hinblick auf die Bedeutung der Aufgabenerfüllung des BayLfV und die Sicherung des Staatswohls nicht ausreichend Rechnung tragen. Die angefragten Informationen würden gerade angesichts ihres spezifischen Detaillierungsgrades in einem so bedeutenden Maße Aufschluss über das mögliche Potenzial der Aktivitäten ausländischer Nachrichtendienste geben, dass eine Weitergabe der besonders geheimhaltungsbedürftigen Informationen auch gegenüber einem eng begrenzten Kreis von Empfängern nicht vertreten werden kann. Je größer der Kreis an Geheimnisträgern ist, umso höher ist die Wahrscheinlichkeit, dass Geheimnisse, sei es absichtlich oder versehentlich, weitergegeben oder ausgespäht werden (vgl. BVerfGE 70, 324 [364]).

- 1.1 Inwieweit sind der Staatsregierung Fälle bekannt, in denen Regierungen anderer Länder gezielt versucht haben, Daten aus der bayerischen Wirtschaft und Wissenschaft abzugreifen (Auflistung nach Datum, Vorfall, Schaden und Land)?**
- 1.2 Wie viele Fälle der Datenspionage sind insbesondere vor chinesischem Hintergrund bekannt (Auflistung nach Datum, Vorfall und Schaden)?**

Zu den Spionageaktivitäten von Regierungen anderer Länder wird allgemein auf den Verfassungsschutzbericht Bayern 2020, S. 309 ff., verwiesen.

Darüber hinaus konnte angesichts der enormen Zunahme digitaler Vernetzung in den letzten Jahren eine Zunahme von APT-Angriffen (APT = Advanced Persistent Threat) beobachtet werden.

Das Handeln von APT-Gruppen basiert zumeist auf der Unterstützung von Staaten und deren Nachrichtendiensten und hat das Ziel, Daten zu stehlen, Abläufe zu sabotieren oder Infrastrukturen anzugreifen.

Im Übrigen wird auf die Vorbemerkung verwiesen.

- 1.3 Geht von China nach Ansicht der Staatsregierung eine besondere Gefahr in Bezug auf die illegale Informationsbeschaffung aus?**

Vor dem Hintergrund unterschiedlicher politischer Systeme und eines nicht von gleichen Wettbewerbsbedingungen geprägten Rahmens ist ein gewisses Gefahrenpotenzial nicht ausgeschlossen.

- 2.1 Welche Maßnahmen ergreift die Staatsregierung, um Wissenschaftseinrichtungen und Unternehmen vor diesen Angriffen zu schützen?**

Die wesentlichen Bausteine bei der Bekämpfung ausländischer (Cyber-)Spionageaktivitäten stellen der gegenseitige Informationsaustausch sowohl im polizeilichen als auch im nachrichtendienstlichen Bereich sowie eine konsequente Strafverfolgung dar.

Ein weiterer wesentlicher Baustein ist die Präventionsarbeit durch Vorträge, Veröffentlichungen, Gespräche sowie Sensibilisierungsmaßnahmen durch das 2013 beim BayLfV gegründete Cyber-Allianz-Zentrum Bayern (CAZ).

Im Bereich der Polizei fungiert die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt als „Single-Point-of-Contact“ für Behörden, Unternehmen, Verbände und sonstige Institutionen, um bei entsprechenden Sachverhalten im Zusammenhang mit der Bekämpfung von Cybercrime als Ersthelfer beratend und unterstützend tätig werden zu können. Um Cyberangriffe zu verhindern bevor sie entstehen, führt die ZAC auch zielgerichtete Präventionsmaßnahmen durch.

- 2.2 Inwieweit fördert die Staatsregierung Digitalisierungskompetenz, Datensicherheit und Cybersecurity, damit sich Unternehmen und Forschungseinrichtungen bestmöglich davor schützen können?**

Die Staatsregierung fördert die Digitalkompetenz, Datensicherheit und Cybersecurity im Rahmen einer Vielzahl von Programmen. Besonders hervorzuheben ist hier die vom Staatministerium für Digitales (StMD) Ende Februar 2019 gestartete Initiative „Online – aber sicher!“ zur Stärkung der Cybersicherheit. Dieses 35 Einzelmaßnahmen umfassende Maßnahmenpaket aller Ressorts unter Federführung des StMD ergänzt die bestehende Bayerische Cybersicherheitsstrategie. Adressaten der Maßnahmen sind gleichermaßen Bürgerinnen und Bürger, Unternehmen, Kommunen und Behörden. So wurde beispielsweise eine Hotline eingerichtet, die bei Cyberangriffen eine direkte Kontaktaufnahme mit Spezialisten des Landeskriminalamtes ermöglicht.

### **2.3 Wie schätzt die Staatsregierung die Umsetzung einer Initiative wie in Baden-Württemberg ein, wo die Landesregierung den Hochschulen Informationssicherheitsbeauftragte zur Seite stellt?**

Die Gewährleistung der Informationssicherheit stellt für die Hochschulen angesichts ihrer internationalen Vernetzung eine besondere Herausforderung dar.

Die Landesregierung von Baden-Württemberg stößt mit einer aktuellen Initiative Maßnahmen an, die in Bayern seit längerem verfolgt und umgesetzt werden.

So haben die bayerischen Hochschulen im Einklang mit entsprechenden fachlichen Empfehlungen der Deutschen Forschungsgemeinschaft (2016) und der Hochschulrektorenkonferenz (2018) ihre IT-Strukturen hinsichtlich Cybersecurity kontinuierlich weiterentwickelt und unter anderem auch Informationssicherheitsbeauftragte eingesetzt.

Diese werden durch die 2016 vom Staatsministerium für Wissenschaft und Kunst (StMWK) im Rahmen des Programms „Digitaler Campus Bayern“ geschaffene Stabsstelle Informationssicherheit an bayerischen staatlichen Universitäten und Hochschulen für angewandte Wissenschaften, angesiedelt an der Hochschule Augsburg, unterstützt. Darüber hinaus haben sich die bayerischen Hochschulen 2020 auf ein Hochschul-Informationssicherheits-Programm (HISP) verständigt, das ein gemeinsames Vorgehen bei der Planung und Festlegung von organisatorischen und technischen Maßnahmen vorsieht. Im nächsten Schritt fördert das StMWK den Aufbau eines hochschulübergreifenden Security Operation Center (SOC), in dem künftig auffällige Ereignisse in den bayerischen Hochschulnetzen zentral analysiert und bei Bedarf Schritte zur Gefahrenabwehr bzw. Schadensminimierung initiiert werden können.

### **3.1 Inwieweit steht die Staatsregierung mit bayerischen Forschungseinrichtungen, Hochschulen sowie Unternehmen in Kontakt, um sich wegen potenzieller Cyberangriffe und Spionage auszutauschen?**

Der Schutz der bayerischen Wirtschaft und Wissenschaft ist Teil des gesetzlichen Präventionsauftrags des BayLfV im Bereich der Spionageabwehr. Das CAZ ist vertraulicher Ansprechpartner für Unternehmen und Forschungseinrichtungen und unterstützt diese mit Informationen, Sensibilisierungen und Beratungsangeboten. Die Kontakte erfolgen sowohl anlassbezogen, das heißt aufgrund von vorliegenden Informationen über die konkrete Bedrohung von Unternehmen und Universitäten durch ausländische Nachrichtendienste, als auch in allgemeiner Form, zum Beispiel durch Vorträge bei Firmen, Verbänden und Hochschulen.

### **3.2 Welche Erkenntnisse liegen dem Landesamt für Sicherheit in der Informationstechnik im Hinblick auf Wissenschafts- und Wirtschaftsspionage aus China vor?**

Dem Landesamt für Sicherheit in der Informationstechnik (LSI) liegen keine Hinweise auf Wissenschafts- und Wirtschaftsspionage aus China vor. Die Ermittlung der Quellen von Cyberangriffen auf die IT-Infrastrukturen der bayerischen Behörden steht auch nicht im Fokus des LSI. Für die Erkennung und Abwehr von Angriffen auf das Bayerische Behördennetz muss unabhängig von deren Provenienz Sorge getragen werden.

### **3.3 Welche anderen staatlichen Stellen gibt es, um Forschung und Wirtschaft vor dem unbefugten Abgreifen von Informationen zu schützen?**

Der Aufbau einer langfristigen Sicherheitspartnerschaft mit den Unternehmen ist im Bereich der IT-Sicherheit von zentraler Bedeutung. Deswegen fördert das Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi) die „Initiative Wirtschaftsschutz“. Es handelt sich hierbei um eine Beratungsinitiative zur Sensibilisierung der Wirtschaft zum Thema Know-how-Schutz und Know-how-Abfluss. Die Initiative wird vom StMWi gemeinsam mit dem StMI bzw. dem BayLfV durchgeführt. Das BayLfV betreibt im Rahmen dieser Initiative das Informationsportal [www.wirtschaftsschutz.bayern.de](http://www.wirtschaftsschutz.bayern.de).

#### **4.1 Welche Sicherheitsvorkehrungen spielen bei der Einstellung von chinesischen Wissenschaftlerinnen und Wissenschaftlern bei Forschungsprojekten und in Unternehmen eine Rolle?**

Spezifische Sicherheitsvorkehrungen bei der Einstellung von chinesischen Wissenschaftlerinnen und Wissenschaftlern bestehen nicht.

Maßgebend sind die tarifvertraglichen und dienstrechtlichen Regelungen, hier insbesondere § 3 Abs. 2 Tarifvertrag für den öffentlichen Dienst der Länder (TV-L), in dem Verschwiegenheits- und Geheimhaltungspflichten normiert sind. Wie bei allen Einstellungen erfolgen unabhängig von der Staatsangehörigkeit eine Überprüfung der Verfassungstreue sowie der Hinweis auf die verschiedenen arbeitsvertraglichen Verpflichtungen.

Einstellungsvoraussetzung ist im Übrigen immer die Erteilung eines Visums durch die deutschen Auslandsvertretungen in China sowie ggf. die Erteilung eines Aufenthaltstitels/einer Arbeitserlaubnis durch die Ausländerbehörde im Inland. Insofern wird auf etwaige Prüfprozeduren der Auslandsvertretungen und zuständigen weiteren Behörden verwiesen.

Ohne konkreten Anlass bzw. spezifische Hinweise auf Spionageabsichten weitergehende Sicherheitsvorkehrungen zu ergreifen, widerspräche dem verfassungsrechtlichen Gleichbehandlungsgrundsatz und dem Allgemeinen Gleichbehandlungsgesetz.

#### **4.2 Welche Sicherheitsvorkehrungen erfolgen hier, damit sichergestellt wird, dass Informationen nicht an unbefugte Dritte weitergegeben werden?**

In Forschungs- und Entwicklungs- bzw. Kooperationsverträgen erfolgt als Sicherheitsvorkehrung üblicherweise eine projektbezogene Verpflichtung auf die Vertraulichkeitsregelungen.

Bei der Verhandlung von Verträgen mit chinesischen Partnern ist insbesondere auch auf die Einhaltung des Exportrechts zu achten; betreffende Professuren werden diesbezüglich sensibilisiert und angehalten, exportrechtliche Vorgaben umzusetzen.

In Verdachtsfällen werden geeignete Maßnahmen ergriffen, etwa in Form einer Meldung an den Verfassungsschutz.

Grundsätzlich werden zum Schutz von Bewerberinnen und Bewerbern bzw. Mitarbeiterinnen und Mitarbeitern vor Diskriminierung keine Maßnahmen ergriffen, die lediglich chinesische Wissenschaftlerinnen und Wissenschaftler betreffen. Die Maßnahmen zum Schutz vor unerlaubter Weitergabe von Informationen gelten für alle Mitarbeiterinnen und Mitarbeiter gleichermaßen.

#### **4.3 Wie viele Einrichtungen und Unternehmen haben den Beratungsdienst des Landesamtes für Verfassungsschutz („Wirtschaftsschutz“: Prävention durch Information) in den vergangenen Jahren in Anspruch genommen?**

Das BayLfV hat im Jahr 2019 an 31 Sensibilisierungsveranstaltungen allgemeiner Art teilgenommen. Darüber hinaus gab es 336 Kontakte wegen des Verdachts potenzieller Cyberangriffe und Spionage gegen bayerische Firmen und Forschungseinrichtungen. Im Jahr 2020 hat das BayLfV an 20 Sensibilisierungsveranstaltungen allgemeiner Art teilgenommen und es gab 189 Kontakte wegen des Verdachts potenzieller Cyberangriffe und Spionage gegen bayerische Firmen und Forschungseinrichtungen.

#### **5.1 Nachdem bekannt wurde, dass die chinesische Regierung hier lebende chinesische Staatsbürgerinnen und Staatsbürger gezielt zur Informationsbeschaffung aufsucht und anzuwerben versucht, welche Maßnahmen hat die Staatsregierung seitdem eingeleitet, um dies zu verhindern?**

#### **5.2 Stehen hier lebende chinesische Staatsbürgerinnen und Staatsbürger diesbezüglich unter Beobachtung?**

#### **5.3 Falls ja, wie viele Personen betrifft das?**

Unklar ist, auf welche Bekanntmachung die Fragesteller abstellen.

Allgemein ist darauf hinzuweisen, dass Ausspäh- und Anwerbeversuche durch ausländische Nachrichtendienste in Deutschland in deren Aufgabenspektrum liegen. Die-

se Versuche werden unter anderem sowohl mit menschlichen Quellen als auch mit technischen Mitteln durchgeführt. Beides geschieht wahlweise offen oder konspirativ.

Das BayLfV kommt im Rahmen seiner Aufgabenzuweisung gemäß Art. 3 Bayerisches Verfassungsschutzgesetz (BayVSG) i. V. m. § 3 Abs. 1 Nr. 2 Bundesverfassungsschutzgesetz (BVerfSchG) der Aufgabe der Sammlung und Auswertung von Informationen über geheimdienstliche Tätigkeiten für eine fremde Macht in Deutschland nach und wird fallbezogen tätig. Werden Fälle in Bayern bekannt, erfolgen Sensibilisierungsgespräche, unter anderem in den Bereichen Wirtschaft und Staatsverwaltung sowie an Hochschulen, Universitäten und Forschungseinrichtungen.

Im Übrigen wird auf den Verfassungsschutzbericht Bayern 2020, S. 307 ff. und auf die Vorbemerkung verwiesen.

**6. Welche Erkenntnisse liegen der Staatsregierung darüber vor, dass die chinesische Regierung offenbar bewusst soziale Netzwerke nutzt, um Informantinnen und Informanten auch in Bayern anzuwerben?**

Es wird auf den Verfassungsschutzbericht Bayern 2020, S. 309 ff. verwiesen.

**7.1 Inwieweit hat die Staatsregierung die chinesischen Nachrichtendienste, Ministry of State Security, Military Intelligence Department, Third Department, im Blick?**

**7.2 Welche Aktivitäten chinesischer Nachrichtendienste (Ministry of State Security, Military Intelligence Department, Third Department etc.) im Freistaat sind der Staatsregierung bekannt?**

Das BayLfV kommt im Rahmen seiner Aufgabenzuweisung gemäß Art. 3 BayVSG i. V. m. § 3 Abs. 1 Nr. 2 BVerfSchG der Aufgabe der Sammlung und Auswertung von Informationen über geheimdienstliche Tätigkeiten für eine fremde Macht in Deutschland nach.

Im Übrigen wird auf den Verfassungsschutzbericht Bayern 2020, S. 309 ff. und auf den Verfassungsschutzbericht des Bundes, S. 291 ff. verwiesen.

**8. Sind der Staatsregierung Fälle bekannt, in denen weitere staatliche Einrichtungen (über den Wissenschaftsbereich hinaus) Ziel von Spionage sind oder waren?**

Es liegen keine Erkenntnisse im Sinne der Fragestellung vor.