

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Raimond Scheirich, Leif-Erik Holm, Dr. Malte Kaufmann, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/3408 –**

Wirtschaftsspionage und Einflussnahme ausländischer Akteure in Deutschland

Vorbemerkung der Fragesteller

Wirtschaftsspionage zählt zu den zentralen sicherheits- und wirtschaftspolitischen Herausforderungen für die Bundesrepublik Deutschland. Nach Angaben des Bundesamtes für Verfassungsschutz nimmt die Zahl der versuchten und erfolgreichen Spionageakte gegen deutsche Unternehmen und Forschungseinrichtungen seit Jahren zu (www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html). Dabei treten insbesondere staatlich gelenkte oder staatlich geduldete Aktivitäten ausländischer Akteure in Erscheinung, die auf den Abfluss von Know-how in strategischen Schlüsseltechnologien, kritischen Infrastrukturen und zukunftsrelevanten Innovationsfeldern zielen.

Zugleich bestehen Hinweise, dass nicht nur klassische nachrichtendienstliche Mittel eingesetzt werden, sondern auch zunehmend Instrumente des sogenannten „Soft Power“-Einflusses, etwa über kulturelle oder wissenschaftliche Kooperationseinrichtungen (www.zeit.de/politik/deutschland/2019-11/konfuzius-institute-china-hochschulen-fdp-kritik, Bundestagsdrucksache 19/24163). In diesem Zusammenhang geraten die in Deutschland ansässigen Konfuzius-Institute, die als Plattformen für chinesische Sprache und Kultur auftreten, regelmäßig in den Fokus öffentlicher Diskussionen. Kritiker verweisen auf institutionelle, organisatorische und finanzielle Abhängigkeiten dieser Institute von der politischen Führung der Volksrepublik China und auf mögliche Einflussnahmen auf Lehre, Forschung und Meinungsfreiheit.

Vor diesem Hintergrund soll die Bundesregierung zu den bestehenden Erkenntnissen, ihrer Bewertung sowie zu getroffenen und geplanten Schutzmaßnahmen Stellung nehmen.

Vorbemerkung der Bundesregierung

Die Antwort zu den Fragen 9 und 20 kann nicht offen erfolgen. Die Einstufung der Antwort auf die Frage als Verschlussache (VS) mit dem Geheimhaltungsgrad „VS-Nur für den Dienstgebrauch“ ist im vorliegenden Fall im Hinblick auf das Staatswohl erforderlich. Nach der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern (BMI) zum materiellen und organisatori-

schen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Frage würde Informationen zur Erkenntnislage, Methodik und Fähigkeiten des Bundesnachrichtendienstes (BND) einem nicht eingrenzenden Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher als „VS-Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Die Antwort zu Frage 2 kann nicht offen erfolgen. Die Einstufung der Antwort auf die Frage als VS mit dem Geheimhaltungsgrad „VS-Vertraulich“ ist im vorliegenden Fall im Hinblick auf Gründe des Staatswohls erforderlich. Nach der VSA sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein können, entsprechend einzustufen.

Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten zur Methodik, Fähigkeiten und zur Erkenntnislage des BND bekannt würden, insbesondere da sich hieraus Rückschlüsse über Aufklärungsansätze und Aufklärungsschwerpunkte ableiten lassen. Insbesondere würde eine Offenlegung Rückschlüsse auf das im BND zu gegen Deutschland gerichteten Spionageaktivitäten vorhandene Wissen erlauben, was für ausländische Nachrichtendienste einen erheblichen Vorteil in ihrer Arbeit gegen die Bundesrepublik bedeuten würde. Ferner könnten entsprechende nachrichtendienstliche Aktivitäten anderer Staaten als Folge angepasst werden und schlimmstenfalls nicht mehr in die Detektion des BND fallen. Eine Beantwortung der angefragten Informationen kann aus diesem Grund nur als VS mit dem Geheimhaltungsgrad „VS-Vertraulich“ erfolgen.

1. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage Deutschlands durch Wirtschaftsspionage (bitte differenziert nach staatlich unterstützten und nichtstaatlichen Akteuren angeben)?

Vor dem Hintergrund zunehmender geopolitischer Rivalitäten und aufgrund der wirtschaftlichen Leistungsfähigkeit sowie Forschungs- und Entwicklungskompetenzen deutscher Wirtschaftsunternehmen ist insgesamt eine erhöhte Gefährdung im Bereich der Wirtschaftsspionage anzunehmen. Neben der strategischen Aufklärung, der verdeckten Beschaffung von militärischen Technologien und Know-how verfolgen staatliche Akteure auch die Vorbereitung gezielter Sabotagehandlungen. Zum Einsatz kommen sowohl cybergestützte als auch realweltliche nachrichtendienstliche Methoden.

Die aktuelle Gefährdungslage Deutschlands durch Wirtschaftsspionage ausgehend von der Russischen Föderation wird als hoch bewertet.

China arbeitet im Bereich der Emerging Technologies (EMT) mit Hochdruck an dem von der Kommunistischen Partei Chinas (KPCh) propagierten „Sprung an die Weltspitze“ – auch unter vielfältiger Nutzung des deutschen Marktes und der deutschen Wissenschaftslandschaft. Dies geschieht durch die (Forschungs-)Güterbeschaffung im Rahmen regulärer Geschäftsbeziehungen, ausländischen Direktinvestitionen oder Wissenschaftskooperationen. Häufig sind solche Beschaffungsaktivitäten weder Gegenstand von Sanktionen oder internationalen Restriktionen noch von nationalen beziehungsweise europäischen Exportbeschränkungen. Mit der Investitionsprüfung steht ein Instrument zur

Überprüfung ausländischer Direktinvestitionen zur Verfügung. Erkennbar ist in vielen Bereichen die Anfälligkeit Deutschlands für Abflüsse hiesiger Hochtechnologie. Da insbesondere EMT mit zivil-militärischem Dual-Use-Charakter das Potenzial haben, zukünftige militärische Auseinandersetzungen in einem Maße zu beeinflussen, das der Wirkung von Massenvernichtungswaffen nahek kommt, ist diese Entwicklung mit Sorge zu betrachten.

Aufgrund der engen Verknüpfung von staatlichen Strukturen und ihren nationalen Wirtschaftsunternehmen lassen sich nichtstaatliche von staatlich motivierten Akteuren nicht zuverlässig unterscheiden.

2. Welche Staaten stuft die Bundesregierung derzeit als besonders aktive Urheber oder Auftraggeber von Wirtschaftsspionage gegen deutsche Unternehmen oder Forschungseinrichtungen ein (bitte mit kurzer Begründung auflisten)?

Wirtschaftsspionage ist durch ein hohes Dunkelfeld und insbesondere auch durch ein sogenanntes doppeltes Dunkelfeld (erstes Dunkelfeld: nicht bekannt gewordene Sachverhalte; zweites Dunkelfeld: von Unternehmen nicht gemeldete Sachverhalte aus z. B. Imageverlustgründen) gekennzeichnet.

Aufgrund der wirtschaftlichen Leistungsfähigkeit sowie Forschungs- und Entwicklungskompetenzen deutscher Wirtschaftsunternehmen steht Deutschland generell im Blickfeld von Wirtschaftsspionage.

Russische Cyberaktivitäten gegen deutsche Unternehmen sind vor allem unter Einfluss des russischen Angriffskrieges auf die Ukraine und der seitens der Bundesrepublik Deutschland geleisteten Unterstützung zur Verteidigung der Ukraine zu betrachten. Daher sind unter anderem die Sektoren Rüstungsindustrie und Logistik besonders im Fokus.

Chinesische Cyberaktivitäten erfolgen großflächig und professionell aus technologischen (beispielsweise Halbleitertechnologie, Marinetchnik), strategischen oder wettbewerbsorientierten Interessen.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

3. Wie viele nachweisbare Fälle oder Verdachtsfälle von Wirtschaftsspionage sind der Bundesregierung in den Jahren 2018 bis 2025 bekannt geworden (bitte nach Jahren aufschlüsseln)?

Es wird auf die Antwort zu Frage 23 verwiesen.

4. Wie hoch war der wirtschaftliche Schaden durch Wirtschaftsspionage in den Jahren 2018 bis 2025 (bitte nach Jahren aufschlüsseln)?

Der Bundesregierung liegen hierzu keine eigenen Zahlen vor. Es wird auf die jährlich erscheinende Studie der BITKOM (www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz) verwiesen.

5. In welchen Wirtschafts- oder Technologiebereichen verzeichnet die Bundesregierung ein erhöhtes Risiko für Wirtschaftsspionage (bitte angeben)?

Ein erhöhtes Risiko für Wirtschaftsspionage durch Russland besteht für die Rüstungsindustrie, den Sektor Luft- und Raumfahrt, bzw. für sämtliche Unter-

nehmen, die auch militärisch nutzbare Technologien herstellen oder erforschen. Im Sachzusammenhang wird auch auf die Antwort zu Frage 2 verwiesen.

Das Bundesamt für Verfassungsschutz (BfV) veröffentlicht Sicherheitshinweise und weitere Erkenntnisse zu relevanten staatlich gelenkten Cyberkampagnen. Ziel ist hier vor allem die breite Sensibilisierung zu Sachverhalten und die Bereitstellung von (technischen) Informationen zur Detektion oder Abwehr entsprechender Angriffe. Bei konkreter Betroffenheit erfolgt eine unmittelbare Sensibilisierung und Weitergabe relevanter Informationen an das betroffene Unternehmen. Neben der bilateralen Abstimmung zwischen den zuständigen Behörden erfolgt eine Koordinierung vor allem im Nationalen Cyberabwehrzentrum, in dem auf Bundesebene alle zuständigen Behörden vertreten sind.

Die chinesische Regierung hat in der Strategie „Made in China 2025“ zehn Zukunftsbranchen identifiziert, in denen China die globale Markt- und Technologieführerschaft anstrebt: Meerestechnik und Schifffahrt, Schienenverkehrstechnik und Eisenbahn, neue Energien und alternative Antriebe, neue Werkstoffe, Landwirtschaft, Medizintechnik, elektrische Ausrüstung, Industrierobotik und Roboterbau, neue Informationstechnologien sowie Luft- und Raumfahrttechnik.

6. Welche Rolle spielen digitale Angriffe und Cyberoperationen bei der Erlangung von wirtschaftlich sensiblen Informationen nach Einschätzung der Bundesregierung?

Aus Sicht der Bundesregierung sind digitale Angriffe und Cyberoperationen ein wichtiges Werkzeug ausländischer Akteure für die Erlangung von wirtschaftlich sensiblen Informationen.

7. Welche Bundesbehörden sind mit der Aufklärung, Prävention und Abwehr von Wirtschaftsspionage befasst, und wie erfolgt die ressortübergreifende Koordinierung dieser Aufgaben?

Die mit der Aufklärung, Prävention und Abwehr von Wirtschaftsspionage befassten Bundesbehörden sind das BMI, das Bundesministerium für Wirtschaft und Energie (BMWE), das Auswärtige Amt (AA), das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR), das BfV, das Bundeskriminalamt (BKA), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), der BND sowie der Generalbundesanwalt beim Bundesgerichtshof (GBA). Zwecks arbeitsteiliger Kooperation beteiligen sich diese Stellen fallbezogen und im Rahmen ihrer jeweiligen Zuständigkeit.

Eine wichtige Rolle spielt hier die Initiative Wirtschaftsschutz. Hier arbeiten Expertinnen und Experten aus den Sicherheitsbehörden sowie Vertreter und Vertreterinnen aus Spitzenwirtschafts- und Sicherheitsverbänden (Bundesverband der Deutschen Industrie e. V. (BDI), Bundesverband der Sicherheitswirtschaft e. V. (BDSW), Deutsche Industrie- und Handelskammer (DIHK), Verband für Sicherheit in der Wirtschaft e. V. (VSW)) und projektbezogen mit weiteren Partnern zusammen.

Die Initiative bietet ein zielgruppenspezifisches Informations- und Beratungsangebot für Unternehmen – auch mit Blick auf hybride Bedrohungen und aktuelle sicherheitsrelevante Entwicklungen. Sicherheitsbehörden und Verbände stehen hierbei in engem fachlichem Austausch mit dem Ziel, adressatengerecht zu sensibilisieren, zu informieren und zu unterstützen. Behördlicherseits koordiniert das BMI alle Maßnahmen zum Wirtschaftsschutz auf Bundesebene.

Es wird im Sachzusammenhang auf die Antwort zu Frage 24 verwiesen.

8. Welche rechtlichen Grundlagen und Befugnisse stehen den Sicherheitsbehörden zur Verfügung, um Wirtschaftsspionage zu verfolgen und zu verhindern und zu sanktionieren?

Die Abwehr und Aufklärung von Wirtschaftsspionage als geheimdienstliche Tätigkeit für eine fremde Macht ist Verfassungsschutzaufgabe nach § 3 Absatz 1 Nummer 2 des Bundesverfassungsschutzgesetzes (BVerfSchG), für die das BfV die Befugnisse nach dem BVerfSchG sowie dem Artikel 10-Gesetz (§ 3 Absatz 1 Nummer 3 G 10) besitzt und zu der es nach § 16 Absatz 1 BVerfSchG auch vorbeugend besonders berät.

Strafbar ist Wirtschaftsspionage, sofern es um die staatlich betriebene nachrichtendienstliche Ausforschung von Wirtschaftsunternehmen geht, speziell nach § 99 des Strafgesetzbuches als geheimdienstliche Agententätigkeit, so dass strafrechtliche Ermittlungen mit den Befugnissen der Strafprozessordnung (StPO) erfolgen können, unter Umständen auch unter Einschluss intensiv eingreifender Maßnahmen nach §§ 100a ff. der StPO. Daneben sind je nach konkretem Sachverhalt eine Vielzahl strafbarer und rechtsgutverletzender Handlungen denkbar, auf die die jeweils dazu einschlägigen allgemeinen Vorschriften des Straf- oder Gefahrenabwehrrechts zur Anwendung gelangen.

9. Welche finanziellen und personellen Ressourcen stehen den zuständigen Behörden zur Bekämpfung von Wirtschaftsspionage zur Verfügung (bitte für das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst, das Bundesamt für Sicherheit in der Informationstechnik, das Bundesministerium des Innern und das Bundesministerium für Wirtschaft und Energie sowie eventuelle Behörden der Bundesländer angeben)?

Bezüglich der in der Fragestellung erbetenen Informationen zu den finanziellen und personellen Ressourcen zur Bekämpfung von Wirtschaftsspionage ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung zum BfV nicht erfolgen kann.

Konkrete Angaben zur Stellenverteilung, die über die im Verfassungsschutzbericht gemäß § 16 Absatz 2 BVerfSchG genannten Strukturdaten hinausgehen, sind – aus Gründen des Staatswohls – nicht angezeigt. Eine Auskunft über die Größenordnung des eingesetzten Personals würde Rückschlüsse auf die Arbeitsweise und Methodik des BfV und insbesondere dessen Aufklärungsfähigkeiten und -tätigkeiten sowie Analysemethoden zulassen. Arbeitsmethoden und technische Fähigkeiten sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags des BfV jedoch besonders schutzwürdig und stellen für die Aufgabenerfüllung des Nachrichtendienstes einen überragend wichtigen Grundsatz dar. Durch eine regelmäßige Abfrage von Mitarbeiterzahlen der einzelnen Fachbereiche des BfV könnten die Entwicklungen des Personalkörpers festgestellt werden. Dies ermöglicht Rückschlüsse auf Arbeitsschwerpunkte des BfV, da die Entwicklung des Personalkörpers in Kontext zu geopolitischen Ereignissen und sicherheitsrelevanter Entwicklungen auf nationaler Ebene gesetzt werden könnten. Dies würde offenlegen, auf welche Ereignisse das BfV reagiert und in seiner Bearbeitung durch die Zuteilung von Personal priorisiert. Ein Bekanntwerden der Mitarbeiterzahlen, beispielsweise gegenüber ausländischen staatlichen Akteuren, könnte dazu führen, dass diese Abwehrstrategien gegen eine eventuelle Bearbeitung durch das BfV etablieren. Dies würde die Erkenntnisgewinnung des BfV erschweren oder in Einzelfällen unmöglich machen. Die Funktionsfähigkeit des BfV wäre dadurch nachhaltig beeinträchtigt,

dies würde einen Nachteil für die Sicherheit der Bundesrepublik Deutschland bedeuten. Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer Relevanz und Sensibilität im Hinblick auf die Bedeutung der nachrichtendienstlichen Aufklärung für die Aufgabenerfüllung des BfV nicht in Betracht. Das Risiko, dass derart sensible Informationen bekannt werden, kann unter keinen Umständen hingenommen werden. Eine Bekanntgabe der erfragten Informationen auch gegenüber einem begrenzten Kreis von Empfängern würde dem Schutzbedürfnis deshalb nicht Rechnung tragen.

Dem BSI stehen keine finanziellen oder personellen Ressourcen speziell zur Bekämpfung von Wirtschaftsspionage zur Verfügung.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

10. Welche Kenntnisse hat die Bundesregierung über die Struktur, Finanzierung und Steuerung der in Deutschland ansässigen Konfuzius-Institute?
11. Welche Bundesländer und Hochschulen beherbergen nach Kenntnis der Bundesregierung derzeit Konfuzius-Institute, und in welcher Rechtsform sind diese organisiert (bitte tabellarisch darstellen)?
12. Welche Stellen oder Institutionen der Volksrepublik China (insbesondere ihrer politischen Führung) sind nach Kenntnis der Bundesregierung an der Finanzierung oder inhaltlichen Steuerung der Konfuzius-Institute in Deutschland beteiligt?
13. Welche Erkenntnisse liegen der Bundesregierung über mögliche Einflussnahmen der Konfuzius-Institute auf Lehrinhalte, Forschungsthemen oder Personalentscheidungen an deutschen Hochschulen vor?
14. Hat die Bundesregierung Bewertungen zu möglichen Verstößen gegen akademische Freiheit oder Wissenschaftsfreiheit im Umfeld der Konfuzius-Institute vorgenommen, und wenn ja, welche?
15. In welcher Weise arbeitet die Bundesregierung ggf. mit den Ländern und Hochschulen zusammen, um mögliche sicherheitsrelevante Risiken im Zusammenhang mit den Konfuzius-Instituten zu bewerten?
16. Welche Gespräche hat die Bundesregierung in den letzten fünf Jahren ggf. mit Vertretern chinesischer Behörden oder Organisationen über die Tätigkeit der Konfuzius-Institute geführt (bitte Zeitpunkt, Teilnehmer und Themenbereich nennen)?
17. Liegen der Bundesregierung belastbare Hinweise auf nachrichtendienstliche Aktivitäten im Umfeld der Konfuzius-Institute oder in deren organisatorischem Umfeld vor?
18. Welche Schlussfolgerungen zieht die Bundesregierung aus ähnlichen Entwicklungen in anderen westlichen Staaten, in denen Konfuzius-Institute geschlossen oder neu strukturiert wurden (z. B. Schweden, Dänemark, Finnland, Vereinigte Staaten von Amerika, vgl. <https://internationalpolitik.de/de/konfuzius-welterfolg>, www.gao.gov/products/gao-24-105981, [https://www.gfbv.de/de/news/universitaet-stockholm-schliesst-chinesisches-konfuzius-institut-6656/#:~:text=Die%20Gesellschaft%20f%C3%97 ProzentB6lker%20\(GfbV\)%20begr%C3%97 ProzentBC%C3%97 Prozent9Ft,Stockholm%20nach%20 ProzentC3%97 ProzentB6ffentlicher%20Kritik%20die%20Schlie%C3%97](https://www.gfbv.de/de/news/universitaet-stockholm-schliesst-chinesisches-konfuzius-institut-6656/#:~:text=Die%20Gesellschaft%20f%C3%97 ProzentB6lker%20(GfbV)%20begr%C3%97 ProzentBC%C3%97 Prozent9Ft,Stockholm%20nach%20 ProzentC3%97 ProzentB6ffentlicher%20Kritik%20die%20Schlie%C3%97), <https://euractiv.de/news/finnland-schliesst-konfuzius-institut-nach-zensur-und-spionagevorwurfen/>)?

26. Wie bewertet die Bundesregierung, insbesondere das Bundesamt für Verfassungsschutz, die Konfuzius-Institute sicherheitsrechtlich, und werden Konfuzius-Institute oder andere von der Volksrepublik China getragene oder mitgetragene Einrichtungen in Deutschland wegen des Verdachts der Wirtschaftsspionage oder vergleichbarer Aktivitäten beobachtet?
28. Welche Erkenntnisse hat die Bundesregierung ggf. über die Personalauswahl, Weisungsgebundenheit und etwaige Rückkehrpflichten von durch die chinesische Seite entsandten Lehrkräften und sonstigem Personal an Konfuzius-Instituten in Deutschland?
29. Welche Erkenntnisse hat die Bundesregierung ggf. über die IT-Infrastruktur der Konfuzius-Institute und über mögliche Zugriffe ausländischer Stellen auf personenbezogene Daten von Studierenden, Kursteilnehmern oder Hochschulangehörigen?
30. In welcher Weise sind ggf. Fälle dokumentiert, in denen Hochschulen oder Bundesländer Kooperationen mit Konfuzius-Instituten aus Gründen der Wissenschaftsfreiheit, Meinungsfreiheit oder Sicherheit eingeschränkt oder beendet haben, und hat sich die Bundesregierung zu diesen Schritten eine eigene Auffassung erarbeitet (bitte ggf. ausführen)?

Die Fragen 10 bis 18, 26 und 28 bis 30 werden im Sachzusammenhang beantwortet.

Die chinesischen Konfuzius-Institute (KI) wurden ursprünglich von der offiziellen außenpolitischen Kulturorganisation HANBAN gesteuert, die dem chinesischen Bildungsministerium unterstellt war. Mitte 2020 wurde das HANBAN als Dachorganisation der KI durch zwei neu gegründete Institutionen, die CHINESE INTERNATIONAL EDUCATION FOUNDATION (CIEF) und das CENTER FOR LANGUAGE EDUCATION AND COOPERATION (CLEC), abgelöst. Die KI sind weiterhin staatlich angebunden. Sämtliche akademische Einrichtungen Chinas sind dem chinesischen Bildungsministerium unterstellt.

Die Bundesregierung führt auf geeigneten Ebenen regelmäßig bilaterale Gespräche mit der chinesischen Seite. Eine systematische Erfassung der dabei besprochenen Themen erfolgt nicht. In ihrer China-Strategie von 2023 hält die Bundesregierung fest: „Deutsche Hochschulen und Wissenschaftsorganisationen sollen sicherstellen, dass Kooperationen mit Konfuzius-Instituten und vergleichbaren chinesischen Partnern den Ansprüchen unseres Bildungs- und Wissenschaftssystems, und dabei insbesondere dem Gedanken der Freiheit von Wissenschaft, Forschung und Lehre, gerecht werden.“ (China-Strategie 4.9., S. 44).

Tabelle 1 – Übersicht Konfuzius-Institute

	Bundesland	Name und Rechtsform	Anbindung an Hochschule
1	Baden-Württemberg	Konfuzius-Institut an der Universität Freiburg e. V.	Albert-Ludwigs-Universität Freiburg
2	Baden-Württemberg	Konfuzius-Institut an der Universität Heidelberg e. V.	An-Institut der Universität Heidelberg
3	Bayern	AUDI-Konfuzius-Institut Ingolstadt e. V.	Technische Hochschule Ingolstadt
4	Bayern	Konfuzius-Institut München e. V.	Nein
5	Bayern	Konfuzius-Institut Nürnberg-Erlangen e. V.	An-Institut der Friedrich-Alexander-Universität Erlangen-Nürnberg
6	Berlin	Konfuzius-Institut an der Freien Universität Berlin e. V.	Freie Universität Berlin

	Bundesland	Name und Rechtsform	Anbindung an Hochschule
7	Bremen	Konfuzius-Institut Bremen e. V.	Hochschule Bremen, Constructor University Bremen
8	Hamburg	Konfuzius-Institut Hamburg e. V.	Nein
9	Hessen	Konfuzius-Institut Frankfurt e. V.	Nein
10	Mecklenburg-Vorpommern	Konfuzius-Institut Stralsund e. V.	Nein
11	Niedersachsen	Akademisches Konfuzius-Institut e. V. an der Georg-August-Universität Göttingen	An-Institut der Universität Göttingen
12	Niedersachsen	Leibniz-Konfuzius-Institut Hannover e. V.	Nein
13	Nordrhein-Westfalen	Konfuzius-Institut Bonn e. V.	An-Institut der Universität Bonn
14	Nordrhein-Westfalen	KI DUS Sprach- und Kultur-Institut gGmbH	Nein
15	Nordrhein-Westfalen	Konfuzius-Institut Metropole Ruhr e. V.	An-Institut der Universität Duisburg-Essen
16	Nordrhein-Westfalen	Konfuzius-Institut Paderborn gGmbH	Nein
17	Rheinland-Pfalz	Konfuzius-Institut Trier e. V.	Nein
18	Sachsen	Konfuzius-Institut Leipzig e. V.	Universität Leipzig
19	Thüringen	Konfuzius-Institut Erfurt e. V.	Nein

Die insgesamt 19 KI in Deutschland sind, wie in Tabelle 1 nachvollziehbar, unterschiedlich organisiert und haben unterschiedliche Kooperationsformen mit in der Tabelle aufgelisteten deutschen Hochschulen. Jedes KI kooperiert darüber hinaus mit einer chinesischen Partneruniversität. Einzelne KI sind in bilaterale Hochschulk Kooperationen eingebunden.

Geleitet werden die Institute von einer Doppelspitze, bestehend aus einem deutschen sowie einem entsandten chinesischen Co-Direktor. Konfuzius-Institute in Deutschland werden überwiegend durch die chinesische Seite finanziert, insbes. über die staatlich kontrollierte CIEF. Diese Mittel decken vor allem Personal, Lehrmaterialien und Programmkosten (Bundestagsdrucksache 19/24163). Die deutschen Partnerhochschulen beteiligen sich i. d. R. durch Sachleistungen wie Räume, Infrastruktur und administrative Unterstützung, seltener durch direkte finanzielle Mittel. Einige Institute ergänzen ihre Einnahmen durch Sprachkurse und Prüfungen.

Die Bundesregierung verfolgt ausländische Versuche der Einflussnahme in Deutschland – über Konfuzius-Institute oder auf anderen Wegen – sehr genau, um potenzielle Risiken für die akademische und wissenschaftliche Freiheit in Deutschland identifizieren und darauf eingehen zu können. Die Bundesregierung sensibilisiert regelmäßig deutsche Hochschulen und Wissenschaftsorganisationen sowie die Länder im Rahmen von Austauschformaten, um sicherzustellen, dass Kooperationen mit Konfuzius-Instituten und chinesischen Partnern aus dem Wissenschaftsbereich den Ansprüchen unseres Bildungs- und Wissenschaftssystems und dabei insbesondere dem Gedanken der Freiheit von Wissenschaft, Forschung und Lehre, gerecht werden. Die Bundesregierung adressiert bei passenden Gelegenheiten wie bspw. den Regierungskonsultationen und

regelmäßigen bilateralen Gesprächen derartige Themen mit chinesischen Stellen.

Die Bundesregierung steht in Bezug auf die KI regelmäßig im Austausch mit relevanten Akteuren auf kommunaler und regionaler Ebene. Zudem wird im Verfassungsschutzbericht seit Jahren öffentlichkeitswirksam auf die o. g. Risiken im Zusammenhang mit KI hingewiesen. Eine Reihe von deutschen Hochschulen hat die Kooperation mit den KI in den vergangenen Jahren aufgekündigt bzw. auslaufen lassen oder überarbeitet, um mögliche Abhängigkeiten zu vermeiden. Die Bundesregierung dokumentiert jedoch keine Fälle, in denen Hochschulen oder Bundesländer Kooperationen mit Konfuzius-Instituten aus Gründen der Wissenschaftsfreiheit, Meinungsfreiheit oder Sicherheit eingeschränkt oder beendet haben.

Die Bundesregierung ist an der Gründung und Ausgestaltung von Konfuzius-Instituten nicht beteiligt.

Auf die Antwort zu Frage 7 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/1465 wird verwiesen.

19. Welche Maßnahmen ergreift die Bundesregierung ggf., um den Schutz sensibler Forschungskooperationen mit chinesischen Partnerinstitutionen sicherzustellen?

In ihrer China-Strategie benennt die Bundesregierung das Ziel, dass „Risiken für die Freiheit von Forschung und Lehre, illegitime Einflussnahme und einseitiger Wissens- und Technologietransfer minimiert“ werden müssen, „die chinesische Politik der zivil-militärischen Fusion setzt unserer Zusammenarbeit Grenzen“.

Die Bundesregierung steht mit den Hochschulen und Forschungseinrichtungen in einem engen Austausch zum Thema Forschungssicherheit gerade in Bezug zu China. Neben den verschiedenen länderagnostischen Maßnahmen zur Stärkung der Forschungssicherheit gibt es zielgerichtete Formate, um Risiken in der Forschungskooperation mit chinesischen Akteuren zu adressieren und Vorkehrungen zu treffen. Darin werden u. a. die verschiedenen chinaspezifischen Aspekte von Forschungsspionage und ungewolltem Wissensabfluss thematisiert sowie Hilfestellungen zur Prüfung von Kooperationen und Stärkung von Forschungssicherheit gegeben. Seit dem Jahr 2020 hat allein das BMFTR, gemeinsam mit dem AA, eine Vielzahl an Informationsveranstaltungen mit Hochschulen sowie der Allianz der Wissenschaftsorganisationen durchgeführt. Themen waren hier u. a. Exportkontrolle, Sicherheitsarchitektur an Hochschulen, Compliance und chinaspezifische Prüfprozesse.

Zum Schutz bereits bestehender sensibler Forschungskooperationen mit chinesischen Partnerinstitutionen trägt das BfV sowohl präventiv als auch fortlaufend durch verschiedene Maßnahmen bei.

Der Austausch mit den wissenschaftlichen Einrichtungen in Deutschland mit Bezug zur Cybersicherheit erfolgt unter anderem auf der Plattform des AK SuWi (Arbeitskreis Sicherheit und Wissenschaft).

Im AK SuWi sind die deutschen Sicherheitsbehörden (u. a. BfV, BND, BSI, Bundesamt für den Militärischen Abschirmdienst (BAMAD), BBK, Bundespolizei (BPoI), BKA, Kommando Cyber- und Informationsraum (KdoCIR)) des Nationalen Cyberabwehrzentrums (NCAZ) vertreten. Die Bundesregierung stellt sicher, dass alle relevanten Informationen unmittelbar an die betreffenden Sicherheitsbehörden im NCAZ weitergeleitet werden. Ferner gewährleistet das BfV den Informationsfluss innerhalb des Verfassungsschutzverbundes. Teilnehmer der wissenschaftlichen Seite ist die Allianz der Wissenschaftsorganisatio-

nen, vertreten durch den Arbeitskreis Informationssicherheit in außeruniversitären Forschungseinrichtungen (AKIF). Der AKIF verfügt über ein Netzwerk bzw. Strukturen, alle öffentlichen geförderten wissenschaftlichen Einrichtungen zu erreichen. Mitglieder der Allianz sind unter anderem die Deutsche Forschungsgemeinschaft (DFG), Fraunhofer-Gesellschaft, Helmholtz-Gemeinschaft Deutscher Forschungszentren, Hochschulrektorenkonferenz, Leibniz-Gemeinschaft und die Max-Planck-Gesellschaft. Ziel des AK SuWi ist die Verbesserung der Cybersicherheit der deutschen Forschungsinstitute sowie die Bündelung der Kooperation zwischen Forschungsinstituten und deutschen Sicherheitsbehörden. So soll unter anderem sichergestellt werden, dass Cyberangriffe mit nachrichtendienstlichem Hintergrund auf wissenschaftliche Einrichtungen besser und schneller detektiert werden können und mögliche schadhafte Auswirkungen reduziert werden. Beispielsweise wird sich im AK SuWi über aktuelle Cyberangriffskampagnen und deren Gefährdungspotential für die Forschung und Wissenschaft ausgetauscht. Daneben kann der AK SuWi auch als Plattform für den Austausch weiterer Informationen auf dem Gebiet der Informationssicherheit genutzt werden.

20. In welcher Weise und durch welche Behörde werden Hochschulen und Forschungseinrichtungen ggf. über Risiken internationaler Kooperationen, insbesondere mit Einrichtungen der Volksrepublik China, informiert und sensibilisiert?

Das aus Mitteln des BMFTR und AA geförderte Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) des Deutschen Akademischen Austauschdienstes (DAAD) unterstützt deutsche Hochschulen bei der Anbahnung, Durchführung und Intensivierung ihrer internationalen Aktivitäten unter komplexen Rahmenbedingungen mit individueller Beratung, vernetzter Expertise und Impulsen für den außenwissenschaftspolitischen Diskurs. Die fünf Themenfelder des Kompetenzzentrums – „Risiko und Sicherheit“, „Rechtliche Rahmenbedingungen“, „Science Diplomacy“, „Forschung, Innovation, Transfer“ sowie „Matchmaking und Internationale Netzwerke“ – werden kontinuierlich weiter ausgebaut. Schwerpunkte der Beratungsarbeit waren im Jahr 2024 u. a. Nachfragen zur Kooperation mit China.

Darüber hinaus ist die Einrichtung einer Nationalen Plattform für Forschungssicherheit auf Bundesebene vorgesehen. Sie soll eine koordinierende und integrierende Funktion übernehmen und vorrangig Wissenschaftseinrichtungen und -organisationen im kollegialen Zusammenspiel mit bestehenden und neuen nationalen, europäischen und internationalen Angeboten und Strukturen dabei unterstützen, Chancen und Risiken vor allem von Forschungsaktivitäten und -kooperationen angemessen bewerten und abwägen sowie Risiken reduzieren zu können.

Das BfV ergreift grundsätzlich verschiedene Maßnahmen zur Sensibilisierung von Bedarfstragenden aus dem Bereich der Forschung und Wissenschaft. Beispielsweise führt das BfV regelmäßig Sensibilisierungen in Form verschiedener Austausch- und Vortragsformate durch. Der Präventionsbereich stellt darüber hinaus zielgruppenspezifische Produkte bereit. Zu diesen gehören die Informationsblätter zum Wirtschaftsschutz, die überblicksartig Themen von dauernder Relevanz beleuchten. Sie dienen als Handreichungen zur Sensibilisierung. Für die Zielgruppe relevant ist z. B. das Infoblatt „Spionage in Wissenschaft und Forschung“.

Die vorgenannten Maßnahmen verfolgen das Ziel, die Zielgruppe Forschung und Wissenschaft für Gefährdungen durch Spionage, darunter u. a. auch solche Risiken, die mit internationalen Kooperationen einhergehen, Sabotage und Ex-

tremismus zu sensibilisieren. Neben der Bundesregierung engagieren sich auch die Landesämter für Verfassungsschutz im Bereich Wissenschaftsschutz.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 19 verwiesen.

21. Plant die Bundesregierung, gesetzliche oder administrative Regelungen zur stärkeren Kontrolle, Transparenz oder Aufsicht über ausländisch finanzierte Kultureinrichtungen und Bildungsk Kooperationen einzuführen, und wenn ja, in welchem Zeitrahmen, und wenn ja, allgemein für alle oder nur jene aus bestimmten Staaten?

Die Bundesregierung plant aktuell keine entsprechenden Regelungen.

22. Über welche Schätzungen oder Daten zur durch Wirtschaftsspionage verursachten jährlichen wirtschaftlichen Gesamtschadenshöhe in Deutschland verfügt die Bundesregierung (bitte differenziert nach Jahren seit 2018 und verursachendem Land angeben)?

Es wird im Sachzusammenhang auf die Antwort zu Frage 3 verwiesen.

23. Wie viele Ermittlungsverfahren und Verurteilungen wegen Spionage, Verrats von Geschäfts- und Betriebsgeheimnissen oder vergleichbarer Delikte im Zusammenhang mit Wirtschaftsspionage wurden seit 2018 nach Kenntnis der Bundesregierung eingeleitet bzw. ausgesprochen (bitte nach Jahren und verursachendem Land differenzieren)?

Im Hinblick auf die Strafverfolgungszuständigkeit des GBA kann eine Beantwortung der Frage wegen des unzumutbaren Aufwandes, der mit der Beantwortung verbunden wäre, nicht erfolgen. Das Bundesverfassungsgericht (BVerfG) hat in ständiger Rechtsprechung bestätigt, dass das parlamentarische Informationsrecht unter dem Vorbehalt der Zumutbarkeit steht (BVerfG, Urteil vom 7. November 2017 – 2 BvE 2/11 –, BVerfGE 147, 50, 147 f.). Danach sind nur die Informationen mitzuteilen, über die die Bundesregierung verfügt oder die sie mit zumutbarem Aufwand in Erfahrung bringen kann. Wirtschaftsspionage ist kein Kriterium, das in den Verfahrensregistern des GBA geführt wird. Erforderlich wäre daher eine händische Auswertung des bis in das Jahr 2018 zurückreichenden immensen Aktenbestandes. Diese Recherche würde die entsprechenden Arbeitseinheiten beim GBA für einen erheblichen Zeitraum in einer Weise beanspruchen, dass diesen eine ordnungsgemäße Erledigung ihrer Ermittlungsaufgaben nicht mehr möglich wäre.

Im Übrigen erteilt die Bundesregierung zu Verfahren, die nicht in die Zuständigkeit des Bundes, sondern in die Zuständigkeit der Länder fallen, aufgrund der Kompetenzverteilung des Grundgesetzes keine Auskünfte.

24. Welche speziellen Unterstützungs-, Beratungs- und Sensibilisierungsangebote hält die Bundesregierung für kleine und mittlere Unternehmen (KMU) sowie Start-ups ggf. bereit, um diese vor Wirtschaftsspionage zu schützen (bitte nach Programmen und Ressorts differenzieren)?

Die Bundesregierung und die ihr nachgeordneten Behörden bieten vielfältige Unterstützung, Beratung und Sensibilisierung für kleine und mittlere Unternehmen (KMU) an.

Das BfV sensibilisiert Unternehmen für Gefährdungen durch Spionage, Sabotage und Extremismus und erfüllt so den gesetzlichen Auftrag aus § 16 Absatz 1 BVerfSchG (präventiver Wirtschaftsschutz). Ziel ist es, dass sich die Wirtschaft effektiv und eigenverantwortlich schützen kann. Dafür entwickelt das BfV zielgruppenspezifische Produkte – wie das SPOC-Magazin, die Sicherheitshinweise für die Wirtschaft oder die Informationsblätter zum Wirtschaftsschutz, und sensibilisiert so auch KMU sowie Start-ups.

Innerhalb des Verfassungsschutzverbundes arbeitet das BfV im Bereich des präventiven Wirtschaftsschutzes eng mit anderen Sicherheitsbehörden zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu den (insbesondere kleinen und mittelständischen) Unternehmen vor Ort.

Darüber hinaus hat sich die „Initiative Wirtschaftsschutz“ zum Ziel gesetzt, zentrale Unternehmenswerte für Deutschland und seine Wirtschaft besser zu schützen. Die beteiligten sicherheitsbehördlichen Akteure stellen Unternehmen, darunter auch KMU und Startups, ihre Expertise im Bereich Wirtschaftsschutz im Rahmen verschiedener Veranstaltungen zur Verfügung.

Das BSI hat im Jahr 2012 gemeinsam mit dem Branchenverband bitkom Deutschlands größtes Privat-Public-Partnership für IT-Sicherheit, die „Allianz für Cybersicherheit“ ins Leben gerufen. Mit der Allianz für Cyber-Sicherheit verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyberangriffen zu stärken. Die zahlreichen Angebote des Netzwerks (u. a. Cyber-Sicherheits-Tage, Cyber-Sicherheits-Web-Talk, Erfahrungs- und Expertenkreisen) werden stetig fortentwickelt (siehe auch: ACS – Allianz für Cyber-Sicherheit – ACS).

Im Übrigen hält das BSI zahlreiche weitere Präventions- und Sensibilisierungsangebote speziell für KMU bereit, welche der Erhöhung der Informationssicherheit in der Wirtschaft und damit auch mittelbar dem Schutz vor Wirtschaftsspionage dienen (siehe auch: BSI – Kleine- und Mittlere Unternehmen).

Um die sichere digitale Transformation des deutschen Mittelstands zu befördern, bündelt das BMWI Unterstützungsangebote unter dem Dach des Förderschwerpunkts Mittelstand-Digital. Eine der beiden Säulen des Förderschwerpunkts ist die Initiative IT-Sicherheit in der Wirtschaft. Sie bietet explizite Unterstützung für kleine und mittlere Unternehmen (KMU), Start-ups und das Handwerk zu Cybersicherheitsfragen. Diese werden dabei unterstützt, Bewusstsein für Cyberrisiken ihres Unternehmens zu entwickeln, ihr Unternehmen gegen die Risiken der digitalen Welt zu schützen und damit ihr Cybersicherheitsniveau zu erhöhen und ihre Resilienz zu stärken.

Im Zentrum der Initiative steht die durch ein Konsortium geleitete Transferstelle Cybersicherheit im Mittelstand. Sie ist die zentrale Anlaufstelle für KMU und Start-ups und übernimmt eine anbieterneutrale Lotsenfunktion, damit sich Unternehmen in der Angebotsvielfalt von Cybersicherheitslösungen zurechtfinden. Die Transferstelle kümmert sich mit einer Fülle an kostenfreien und anbieterneutralen Tools und Angeboten von der Prävention über Detektion bis hin zur Reaktion bundesweit um die Sicherheitsanliegen der Unternehmen.

Darüber hinaus bietet die Initiative IT-Sicherheit in der Wirtschaft ergänzende themenspezifische Fokusprojekte (jeweils Laufzeiten zwischen 6 bis 36 Monate), die sich aktuellen praxisprozessbezogenen und regulatorischen Herausforderungen widmen, wie zum Beispiel den Anforderungen aus der NIS2-Richtlinie und ihrem nationalen Umsetzungsgesetz oder dem Cyber Resilience Act (CRA).

25. Welche Vorgaben zur Sicherheitsüberprüfung und zum Schutz sensibler Informationen bestehen bei der Vergabe von Bundesmitteln für gemeinsame Forschungsprojekte mit Partnerinstitutionen aus Staaten mit erhöhtem Spionagerisiko, insbesondere der Volksrepublik China?

Die Vorgaben zu Sicherheitsüberprüfungen sowie zum Schutz von als VS eingestuften Informationen ergeben sich aus dem Sicherheitsüberprüfungsgesetz (SÜG) sowie den Allgemeinen Verwaltungsvorschriften nach § 35 SÜG, insbesondere der VSA.

27. Wie bewertet die Bundesregierung, insbesondere das Bundesamt für Verfassungsschutz, ausländische, von Staaten getragene oder mitgetragene Vereine, Stiftungen sowie Kultur- und Bildungseinrichtungen in Deutschland sicherheitsrechtlich, und werden derartige Einrichtungen ausländischer Staaten in Deutschland wegen des Verdachts der Wirtschaftsspionage oder vergleichbarer Aktivitäten beobachtet (bitte nach Herkunftsstaat und Art der Einrichtung aufschlüsseln)?
33. Nach welchen Kriterien bewertet die Bundesregierung, insbesondere das Bundesamt für Verfassungsschutz, ob ausländische, von Staaten getragene oder mitgetragene Vereine, Stiftungen sowie Kultur- und Bildungseinrichtungen in Deutschland ein sicherheitsrelevantes Risiko im Hinblick auf Wirtschaftsspionage oder unzulässige Einflussnahme darstellen (bitte die maßgeblichen Prüfkriterien und Rechtsgrundlagen darstellen)?

Die Fragen 27 und 33 werden im Sachzusammenhang beantwortet und in Bezug auf „von der Volksrepublik China getragene oder mitgetragene Einrichtungen in Deutschland“ gebündelt wie folgt beantwortet.

Grundsätzlich erfolgt eine Bewertung der von ausländischen Staaten getragenen oder mitgetragenen Einrichtungen ausgehenden sicherheitsrelevanten Risiken entlang der Frage, ob diese sicherheitsgefährdende oder geheimdienstliche Tätigkeiten i. S. d. § 3 Absatz 1 Nummer 2 BVerfSchG entfalten.

31. Hat die Bundesregierung Leitlinien oder Empfehlungen für Hochschulen erarbeitet, wie bestehende Kooperationen mit Konfuzius-Instituten risikominimierend umgestaltet oder – falls erforderlich – geordnet beendet werden können?

Auf die China-Strategie 4.9. wird verwiesen.

32. Welche vergleichbaren Risiken sieht die Bundesregierung im Hinblick auf andere ausländisch finanzierte Kultur- und Bildungseinrichtungen, und in welcher Weise werden diese Risiken ggf. adressiert?

Auf die Antwort zu Frage 27 wird verwiesen.

34. Plant die Bundesregierung, die Strukturen der Cyberabwehr in Bund und Ländern zu vereinheitlichen bzw. weiter zu harmonisieren, und wenn ja, welche organisatorischen, rechtlichen und technischen Maßnahmen sind hierzu konkret vorgesehen?

Durch den föderalen Staatsaufbau der Bundesrepublik Deutschland ist Bund und Ländern die eigenständige Wahrnehmung der Aufgaben zur Cyberabwehr übertragen. Im Rahmen dessen stimmt sich die Bundesregierung mit den Län-

dern u. a. im IT-Planungsrat fortlaufend zu Fragen der Informationssicherheit und Cyberabwehr mit dem Ziel einer Vertiefung der Zusammenarbeit ab.

35. Inwieweit erhebt die Bundesregierung statistisch, in welchen Fällen erfolgreiche Cyberangriffe auf Hochschulen und Forschungseinrichtungen zu Abflüssen sensibler Forschungsdaten oder Technologiewissen führen, und wie werden diese Erkenntnisse systematisch ausgewertet?

Die Bundesregierung erhebt keine entsprechenden Daten. Eine Verpflichtung zur Meldung von Cyberangriffen an Bundesbehörden besteht nicht. Dazu wird auf die Vorbemerkung der Bundesregierung in der Antwort zur Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/12259 verwiesen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.