Baden-Württemberg
Ministerium des Inneren,
für Digitalisierung und Kommunen

Innenministerium | Willy-Brandt-Str. 41 | 70173 Stuttgart

Präsidentin des Landtags
von Baden-Württemberg
Frau Muhterem Aras MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Datum: 12.02.2025

nachrichtlich:
Staatsministerium
Ministerium für Wissenschaft, Forschung und Kunst
Ministerium für Wirtschaft, Arbeit und Tourismus

Antrag des Abgeordneten Nico Weinmann u. a. FDP/DVP

- **Gefahren chinesischer Einflussnahme und Spionage für das Land Baden-Württemberg**
- **Drucksache 17/8147, Schreiben vom 22.01.2025**

Sehr geehrte Frau Landtagspräsidentin,

das Ministerium des Inneren, für Digitalisierung und Kommunen nimmt zu dem Antrag im Einvernehmen mit dem Ministerium für Wissenschaft, Forschung und Kunst und dem Ministerium für Wirtschaft, Arbeit und Tourismus und wie folgt Stellung:

Der Landtag wolle beschließen,
die Landesregierung zu ersuchen

zu berichten,

Willy-Brandt-Straße 41
70173 Stuttgart
E-Mail: poststelle@im.bwl.de
Telefon: +49 711 231-4

Homepage: im.baden-wuerttemberg.de
Serviceportal: service-bw.de
Datenschutz: im.baden-wuerttemberg.de/datenschutz

Vorbemerkung:

Weite Teile der erbetenen Informationen berühren in besonderem Maße das Staatswohl und können nach sorgfältiger Abwägung zwischen dem verfassungsrechtlich zu gewährleistenden Informationsinteresse des Landtags und dem öffentlichen Interesse an der Geheimhaltung von Informationen nicht bzw. nur eingeschränkt in einem gesonderten VS-NfD eingestuften Stellungnahme-Teil dargestellt werden, auf den hiermit verwiesen wird. Die Einstufung von Teilen der Stellungnahme als Verschlusssache ist erforderlich, da eine Offenlegung Rückschlüsse auf die Bearbeitungsschwerpunkte sowie den Kenntnisstand des Landesamtes für Verfassungsschutz Baden-Württemberg (LfV) zum Agieren chinesischer Nachrichtendienste in Baden-Württemberg ermöglichen würde. Hierdurch könnten die ausländischen Akteure Abwehrstrategien entwickeln und dadurch die Erkenntnisgewinnung des LfV erschweren oder in Einzelfällen unmöglich machen. Dadurch könnte die Funktionsfähigkeit des LfV und damit auch die Sicherheit des Landes nachhaltig beeinträchtigt werden.

1. *inwiefern es in den letzten zehn Jahren Hinweise, Verdachtsfälle oder gar gesicherte Nachweise chinesischer Einflussnahme bzw. Spionageaktivitäten, insbesondere von chinesischen Botschaften durch chinesische Geheimdienste betrieben, in Baden-Württemberg gegeben hat, beispielsweise in den Bereichen Technologie, Forschung, Wissenschaft, Medizin, Waffentechnik usw., zumindest unter Darstellung des Zeitpunkts sowie des betroffenen Ressorts der jeweiligen Vorfälle;*

4. *wie sich nach ihrer Einschätzung versuchte oder gar erfolgreiche Spionageaktivitäten aus China regelmäßig darstellen, zumindest unter geeigneter Darstellung der beobachteten Vorgehensweisen und Ziele;*

10. *wie sie die Gefahren einschätzt, wonach chinesische Agenten in Baden-Württemberg gezielt auf junge Talente oder andere in der Forschung, Wirtschaft, Waffenindustrie usw. Tätige abzielen, um diese für Spionagezwecke zu rekrutieren;*

Zu 1., 4. und 10.:

Zu den Ziffern 1, 4 und 10 wird wegen des Sachzusammenhangs gemeinsam Stellung genommen. Es wird auf den VS-NfD-eingestuften Teil der Stellungnahme hingewiesen.

Eine detaillierte Aufstellung der Hinweise und Verdachtsfälle der letzten zehn Jahre ist aufgrund der Kürze der für die Bearbeitung zur Verfügung stehenden Zeit nicht möglich.

Vor diesem Hintergrund kann insbesondere die Fragestellung gemäß Ziffer 1. nur auf einem abstrakten Niveau beantwortet werden.

Die Erkenntnisse des LfV in Bezug auf den Modus Operandi der chinesischen Nachrichtendienste gehen maßgeblich auf nachrichtendienstliche Hinweise und Analysen des Bundesamtes für Verfassungsschutz (BfV) und des Bundesnachrichtendienstes (BND) zurück. Diese Berichterstattung erfolgt regelmäßig in Berichten oder Schreiben, die mit dem Geheimhaltungsgrad „GEHEIM“ eingestuft sind. Erkenntnisse daraus können aus Geheimhaltungsgründen daher nicht dargestellt werden.

Die wirtschaftlichen und wissenschaftlichen Ambitionen Chinas, die in der „Made in China 2025“-Strategie definiert sind, begründen das chinesische Interesse an sensiblen Informationen aus den Bereichen Wirtschaft, Wissenschaft und Technik. Die Volksrepublik China strebt bis zu ihrem 100-jährigen Bestehen im Jahr 2049 eine weltweite Führungsrolle in maßgeblichen Zukunftstechnologien an. Zur Erreichung dieser ambitionierten Ziele sieht sie auch den Einsatz von Spionage als legitimes Mittel.

Beim Agieren chinesischer Nachrichtendienste ist kein gleichbleibendes, feststehendes Muster erkennbar; auch nicht mit Blick auf die Altersstruktur der von chinesischen Nachrichtendiensten fokussierten Personenkreise. Vielmehr nutzen die chinesischen Nachrichtendienste Spionage, Einflussnahme und transnationale Repression in gegenseitiger Wechselwirkung und flexibel zur Erreichung der oben genannten Ziele.

Die Cyberabwehr im LfV ist durch ihren gesetzlichen Auftrag für die Aufklärung und Abwehr von Cyberangriffen zuständig, die einen mutmaßlich nachrichtendienstlichen Hintergrund aufweisen. Hauptaufgaben der Cyberabwehr sind die frühzeitige Angriffserkennung, die technische Analyse zur Angriffsmethodik, die Erkenntnisgewinnung über mögliche Urheber sowie Präventions- und Sensibilisierungsmaßnahmen.

Im Rahmen dieses gesetzlichen Auftrags bearbeitet die Cyberabwehr regelmäßig Cyberangriffe, die mutmaßlich staatlichen Akteuren aus China zugeordnet werden können, wobei sich diese Angriffe häufig gegen Forschungseinrichtungen staatlicher Institutionen in Baden-Württemberg richten. Aber auch hiesige Wirtschaftsunternehmen stehen unverändert im Fokus chinesischer Cyberakteure.

Für Angriffe im Cyberraum setzt China – wie auch andere Staaten – verschiedene Cybergruppierungen ein. Diese werden allgemein als APT-Gruppen („Advanced Persistent Threat“, „fortgeschrittene, andauernde Bedrohung“) bezeichnet und verschleiern die

wahre Identität des Angreifers. APT-Angriffe zeichnen sich durch einen sehr hohen personellen wie finanziellen Ressourceneinsatz sowie erhebliche technisch-methodische Fähigkeiten aus und sind nur sehr schwer zu entdecken. Mit diesen Angriffen gehen zu Beginn einer Attacke oftmals ausgefeilte manipulative Methoden (Social Engineering) einher, um Menschen zu einem bestimmten sicherheitskritischen Verhalten zu verleiten. Außerdem verwenden APT vielfach sogenannte Spear-Phishing-E-Mails, die passgenau auf die Interessenlagen weniger Empfänger oder Einzelpersonen zugeschnitten sind, um z. B. mittels versteckt integrierter oder angehängter Schadsoftware IT-Systeme zu kompromittieren und so letztlich unbemerkt Datenabflüsse zu generieren.

Eine sorgfältige Abwägung zwischen dem parlamentarischen Informationsrecht und dem öffentlichen Interesse an der Geheimhaltung der genauen Fallzahlen und deren Hintergründe führt zu dem Ergebnis, dass operative Details, zu denen auch konkrete Fallzahlen von Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund gehören, im Rahmen dieser Beantwortung nicht dargestellt werden können. Informationen zur Anzahl der festgestellten Fälle und zu den betroffenen Stellen im Land sind Verschlusssachen mit den Geheimhaltungsgraden „VS-VERTRAULICH“ oder höher, weshalb hierzu keine Angaben gemacht werden können.

2. *inwieweit nach ihrer Einschätzung chinesische Diplomaten oder chinesische Firmen möglicherweise als Deckmantel für Spionageoperationen in Baden-Württemberg tätig sind oder innerhalb der letzten zehn Jahre waren;*

Zu 2.:

Nach hiesiger Bewertung gehört es zum Modus Operandi ausländischer Nachrichtendienste, Diplomaten und als Firmenvertreter getarnte Nachrichtendienstmitarbeiter für Spionageoperationen zu nutzen. Dies gilt grundsätzlich auch für chinesische Nachrichtendienste und auch für deren Agieren in Baden-Württemberg.

3. *inwieweit ihr bekannt ist, dass in diesem Zeitraum versucht wurde, beispielsweise über Telegram, soziale Medien usw., sogenannte „low level agents“ oder „Wegwerfagenten“ zu rekrutieren, zumindest unter Einordnung der von diesen ausgehenden potenziellen Gefahren sowie der bekannten Zahl solcher Vorgänge und der näherungsweisen Einordnung einer Dunkelziffer;*

Zu 3.:

Es wird auf den VS-NfD-eingestuften Stellungnahme-Teil verwiesen.

Allgemein kann hier lediglich ausgeführt werden, dass als sog. „low-level-agents“ nicht nachrichtendienstlich geschulte (in der Regel junge) Personen bezeichnet werden, die insbesondere über soziale Medien und Messenger-Dienste kurzfristig zur Erfüllung konkreter Aufträge rekrutiert werden.

5. *inwieweit ihr in diesem Zeitraum unbefugte Datenübertragungen von Unternehmen oder Behörden aus Baden-Württemberg nach China bekannt sind, zumindest unter Darstellung der jeweiligen Fälle im Hinblick auf den Zeitpunkt sowie den Inhalt der jeweiligen Fälle;*

7. *wie sich in den letzten zehn Jahren die Zahl von (mutmaßlichen) Cyberangriffen aus China auf baden-württembergische Infrastrukturen, Firmen, Behörden usw. entwickelt hat, zumindest unter Darstellung des Zeitpunkts, des Ziels sowie der Einordnung, ob der Angriff erfolgreich war oder ganz bzw. teilweise abgewehrt werden konnte;*

Zu 5. und 7.:

Zu den Ziffern 5 und 7 wird wegen des Sachzusammenhangs gemeinsam Stellung genommen.

Staatlich gesteuerte chinesische Cyberakteure gehören seit jeher zu den aktivsten Angreifern im Cyberraum in Baden-Württemberg. In den letzten zehn Jahren wurden kontinuierlich Cyberspionageangriffe auf baden-württembergische Infrastrukturen, Unternehmen und Behörden mit mutmaßlich chinesischem Hintergrund registriert. Wie bereits dargestellt, sind konkrete Fallzahlen und Details zu Fallbearbeitungen als Verschlusssachen mit den Geheimhaltungsgraden „VS-VERTRAULICH“ bzw. „GEHEIM“ eingestuft und können im Rahmen dieses Antrags nicht dargestellt werden.

6. *inwieweit es eine erhöhte Zahl von chinesischen Staatsbürgern in bestimmten Bereichen wie beispielsweise der IT-Industrie oder der Luft- und Raumfahrttechnik gibt, die mit Spionage in Verbindung stehen könnten;*

Zu 6.:

Hierzu liegen keine Erkenntnisse vor. Die Spionage- und Cyberabwehr des LfV führt keine anlassunabhängige Beobachtung von Personen oder Organisationen durch. Gemäß ihrem gesetzlichen Auftrag wird die Spionage- und Cyberabwehr nur bei Vorliegen tatsächlicher Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetztes für eine fremde Macht tätig.

8. *inwieweit sie spezielle Maßnahmen zur Abwehr von insbesondere chinesischen Spionageaktivitäten ergreift, zumindest unter ausführlicher Darstellung derselben;*

Zu 8.:

Die Spionage- und Cyberabwehr des LfV stellt eine kontinuierliche Bearbeitung sämtlicher Verdachtsfälle gemeinsam mit ihren Partnern im Verfassungsschutzverbund sicher. Hierzu stehen dem LfV eine Vielzahl gesetzlich definierter nachrichtendienstlicher Mittel zur Verfügung.

Zudem stellen die Spionage- und Cyberabwehr sowie der Behörden- und Wirtschaftsschutz des LfV ein umfassendes Angebot an Präventionsmaßnahmen bereit und tragen so zu einem effektiven Schutz vor Spionage und Sabotage bei. Dieses Präventionsangebot richtet sich insbesondere an die Politik und Verwaltung, an die Wissenschaft und Forschung und an die Privatwirtschaft.

Es gliedert sich in anlassbezogene und allgemeine Beratungsformate. Präventionsangebote dienen regelmäßig der Sensibilisierung relevanter privater und öffentlicher Stellen, um deren Resilienz zu stärken und um zu einer erhöhten Detektionsfähigkeit des LfV beizutragen, indem Verdachtsmomente frühzeitig mit dem LfV geteilt werden.

Liegt der konkrete Verdacht eines nachrichtendienstlich gesteuerten Cyberangriffs vor oder besteht die Gefahr, dass eine bislang unbekannte Schwachstelle in einer Software von staatlich gesteuerten oder beeinflussten Akteuren ausgenutzt werden könnte, verfasst die Cyberabwehr anlassbezogene Warnmeldungen und sensibilisiert möglicherweise gefährdete Stellen im Land passgenau und individuell.

Im Zuge der anlassunabhängigen Beratung bietet die Spionage- und Cyberabwehr des LfV spezielle Vorträge bei Multiplikatoren, wie beispielsweise Unternehmensverbänden,

zum Vorgehen ausländischer Nachrichtendienste an, erstellt Handreichungen mit Hinweisen und Handlungsempfehlungen und veröffentlicht regelmäßig Sicherheitshinweise für IT-Fachkräfte auf der Homepage des LfV. Diese Sicherheitshinweise beschäftigen sich jeweils mit einem aktuellen Thema aus dem Bereich der Cybersicherheit und richten sich speziell an IT-Sicherheitsverantwortliche in Unternehmen, staatlichen Stellen und Forschungseinrichtungen.

Die gesamte Präventionsarbeit der Spionage- und Cyberabwehr des LfV erfolgt dabei in enger Zusammenarbeit mit dem Wirtschaftsschutz im LfV, mit anderen Behörden im Verfassungsschutzverbund und mit den Sicherheitsbehörden des Landes, insbesondere dem Landeskriminalamt Baden-Württemberg (LKA) und der Cybersicherheitsagentur Baden-Württemberg (CSBW).

9. *welche Kooperationen zwischen baden-württembergischen Universitäten und chinesischen Institutionen nach ihrer Kenntnis bestehen, zumindest unter Darstellung ihrer Bewertung derselben unter Sicherheitsaspekten;*

Zu 9.:

Das Ministerium für Wissenschaft, Forschung und Kunst hat Kenntnis von 225 Kooperationen (Stand 27.01.2025) zwischen baden-württembergischen Hochschulen und chinesischen Institutionen. Es besteht keine Anzeigepflicht für Kooperationen im Hochschulbereich. Die Kooperationen der Hochschulen sind in der Anlage abgebildet.

Eine Bewertung von Hochschulkooperationen erfolgt in der Verantwortung der jeweiligen Hochschule. Dort obliegt sie im ersten Schritt den Projektbeteiligten, die dabei nach den hochschulinternen Prozessen vorgehen. Anlassbezogen beziehen diese hochschulintern die Exportkontrollbeauftragten, das Justiziariat, die Personalabteilung und das Rektorat ein. Darüber hinaus werden im Bedarfsfall das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), das LfV und weitere Gremien eingebunden, die mit einer umfassenderen Expertise oder in einem Peer-Review-Prozess die Projekte bei der Evaluierung potentieller Risiken unterstützen.

Spezifische Maßnahmen bestehen im Land hinsichtlich drittmittelfinanzierter Forschungsprojekte. Konkret besteht nach § 41 a Landeshochschulgesetz (LHG) (Transparenz der Drittmittelforschung) die Pflicht für die Hochschulen, ein Vorhabenregister über

drittmittelfinanzierte Forschungsvorhaben zu führen. Konkretisiert werden diese Regelungen durch die Verwaltungsvorschrift des Wissenschaftsministeriums und die zugehörigen Hinweise vom 06.03.2024 zur Annahme und Verwendung von Mitteln Dritter zu §§ 13, 41 und 41 a LHG (Drittmittelrichtlinien – DMRL, Az. MWK11-0415.2-1/1/1).

Wissenschaftliche Kooperationen mit Hochschulen und Forschungseinrichtungen bieten im Allgemeinen die Möglichkeit des Technologie- und Know-how-Transfers. Solche Transfers müssen nicht zwingend nachrichtendienstlich motiviert sein. Bekannt ist jedoch, dass der chinesische Staat gezielt rechtliche Grauzonen, ein mangelndes Risikobewusstsein sowie die in Deutschland verfassungsrechtlich garantierte akademische Freiheit ausnutzt.

11. *welche Rolle die App TikTok im Zusammenhang mit chinesischer Einflussnahme, Spionage bzw. Datenabgriffen nach ihrer Einschätzung spielt.*

Zu 11.:

Aufgrund der großen Reichweite und hohen Benutzerzahl der App TikTok ist nahezu sicher, dass fremde Mächte versuchen, diese App für Einflussnahmeoperationen zu verwenden, darunter wahrscheinlich auch die Nachrichtendienste der Volksrepublik China.

Wie bereits in der Stellungnahme zum Antrag der Abg. Daniel Karrais u. a. (FDP/DVP), „TikTok – Chancen und Risiken für die politische Kommunikation“, Drucksache 17/6481, dargelegt, besteht bei der Verwendung von Apps und sozialen Netzwerken die Möglichkeit, dass Anbieter versuchen, mehr personenbezogene Daten zu erlangen, als für die Bereitstellung der Inhalte technisch erforderlich wäre. Die Anbieter begründen dies damit, dass personenbezogene Daten monetarisiert werden müssten, wenn die Bereitstellung der eigentlichen Dienste kostenlos ist.

Die App TikTok verlangt im Rahmen des Installationsprozesses zahlreiche Zugriffsrechte, u. a. auf Mikrofon, Kamera und Ortungsdienste. Zwar stellt TikTok als soziales Netzwerk Dienste bereit, die diese Art von Berechtigungen erfordern. Der Cyberabwehr des LfV liegen jedoch Erkenntnisse vor, dass die App darüber hinaus beim iOS-Betriebssystem von Apple-Geräten bei jedem Start der App unterschiedliche Positionsdaten an Backend-Server des chinesischen Herstellers ByteDance sendet. Bei einem Backend-Server handelt

es sich um ein System zur Verarbeitung von Daten auf leistungsfähigeren Rechnern im Hintergrund. TikTok begründet die Übertragung von Daten an den Backend-Server damit, dass durch die Erhebung der Positionsdaten den Nutzerinnen und Nutzern zielgerichtete, ortsbezogene Informationen angezeigt werden können.

Mit freundlichen Grüßen

gez. Thomas Strobl
Minister des Inneren, für Digitalisierung und Kommunen

Anlage
Tabelle - Kooperationen baden-württembergischer Hochschulen mit chinesischen Institutionen