Deutscher Bundestag **Drucksache 19/22678**

19. Wahlperiode 17.09.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Jens Beeck, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/21948 –

Spionage in Deutschland

Vorbemerkung der Fragesteller

Die Bundesrepublik Deutschland steht im Fokus des Interesses ausländischer Regierungen und ihrer Nachrichtendienste. Die verdeckte Informationsbeschaffung über politische und strategische Vorgänge ist dabei ebenso gängig wie Spionageaktivitäten in Wirtschaft und Wissenschaft oder auch die Sabotage kritischer Infrastrukturen. Das Bundesamt für Verfassungsschutz (BfV) warnt im Verfassungsschutzbericht 2019: „Die negativen Folgen von Spionage sind vielfältig. Dazu zählen unter anderem beeinflusste demokratische Willensbildungsprozesse, vorab bekannt gewordene vertrauliche diplomatische Verhandlungspositionen und Verstöße gegen Recht und Gesetz. Die Ausforschung und Unterwanderung oppositioneller Gruppen aus Drittstaaten durch ausländische Dienste in Deutschland stellt eine weitere Beeinträchtigung der nationalen Souveränität dar. Aber auch der Know-how-Verlust sowie die betriebs- und volkswirtschaftlichen Schäden sind immens“ (s. Bundesamt für Verfassungsschutz: Verfassungsschutzbericht 2019, S. 282).

In den vergangenen Jahren wurden auch gewalttätige Aktivitäten ausländischer Nachrichtendienste in Deutschland bekannt. Im Jahr 2017 wurde laut Presseberichten ein vietnamesischer Staatsbürger durch den Geheimdienst des Landes aus Berlin nach Hanoi verschleppt (vgl. https://www.spiegel.de/politik/deutschland/berlin-entfuehrung-von-thrin-xuan-thanh-mitten-in-berlin-verschleppt-a-1161188.html). Am 18. Juli 2019 wurde der georgische Staatsangehörige tschetschenischer Abstammung Tornike K. im Kleinen Tiergarten in Berlin-Moabit erschossen. Der Generalbundesanwalt (GBA) hat am 18. Juni 2020 Anklage wegen Mordes gegen den russischen Staatsbürger Vadim K. alias Vadim S. erhoben. Er soll laut Presseberichten den Auftrag für den sogenannten Tiergarten-Mord durch staatliche Stellen der Zentralregierung der Russischen Föderation erhalten haben (vgl. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/aktuelle/Pressemitteilung-vom-18-06-2020.html).

Derweil machen Cyberspionage und Cybersabotage einen wesentlichen Teil ausländischer, nachrichtendienstlicher Aktivitäten zum Nachteil der Bundesrepublik Deutschland aus. Im Verfassungsschutzbericht für das Jahr 2019 warnt das BfV angesichts „der weiterhin voranschreitenden Entwicklung zur Digitalisierung und Vernetzung unserer Gesellschaft“ vor einer vergrößerten

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 17. September 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

„Bedrohungslage durch Cyberspionage und Cybersabotage“ (s. Bundesamt für Verfassungsschutz: Verfassungsschutzbericht 2019, S. 283). Viele Aktivitäten im Bereich der Cyberspionage gegen deutsche Stellen gehen demnach von den Nachrichtendiensten der Russischen Föderation und der Volksrepublik China aus (vgl. ebd.). Der Ursprung eines schwerwiegenden Hackerangriffs auf den Deutschen Bundestag im Jahr 2015 geht mutmaßlich auf die Kampagne „APT28“ bzw. „Fancy Bear“ zurück, die dem russischen Militärgeheimdienst GRU zugerechnet wird. Der Generalbundesanwalt erließ in der Sache im Mai 2020 einen Haftbefehl gegen einen russischen Staatsangehörigen (vgl. https://www.tagesschau.de/investigativ/ndr-wdr/hacker-177.html). Erst kürzlich wurde ein Cyberangriff auf die BwFuhrpark Service GmbH, ein Tochterunternehmen der Bundeswehr, das auch den Fahrdienst des Deutschen Bundestages betreibt, bekannt (vgl. https://www.sueddeutsche.de/politik/cyberkriminalitaet-hackerangriff-auf-fahrdienstleister-des-bundestages-1.5000359).

1. Wie schätzt die Bundesregierung die aktuelle Bedrohungslage durch Spionage sowie die Schwerpunkte ausländischer Spionageaktivitäten in Deutschland ein?

Die Bedrohungslage für Deutschland durch Spionage, staatliche Einflussnahme und andere nachrichtendienstliche Aktivitäten verschärft sich in den vergangenen Jahren kontinuierlich. Geopolitisch relevante Konflikte aus verschiedenen Teilen der Welt werden in Deutschland und Europa ausgetragen. Dementsprechend sind Nachrichtendienste vieler Staaten hierzulande verstärkt aktiv und unterstützen mit vielfältigen Mitteln die Interessen ihrer Herkunftsländer.

2. Wie haben sich in den vergangenen fünf Jahren ausländische Spionageaktivitäten in Deutschland mit der Zielsetzung
   a) der Informationsbeschaffung über politische und administrative Vorgänge und Erkenntnisse,
   b) der Informationsbeschaffung und der Einflussnahme auf staatliche Entscheidungsträger,
   c) der Wirtschaftsspionage,
   d) der Wissenschaftsspionage,
   e) der Sabotage beispielsweise im Bereich von kritischer Infrastruktur sowie
   f) der Proliferation entwickelt?

Die Fragen 2 bis 2f werden im Sachzusammenhang beantwortet.

Die Aktivitäten fremder Nachrichtendienste in der Bundesrepublik Deutschland haben in den vergangenen fünf Jahren zugenommen. Besonders hervorzuheben sind hierbei die Zunahme sicherheitsgefährdender Einflussnahme-Aktivitäten anderer Staaten und das Vorgehen gegen Oppositionelle anderer Staaten, die sich in Deutschland befinden. Diese sind regelmäßig Ziel von Ausspähungen und zum Teil Opfer weitergehender Aktionen – bis hin zu Maßnahmen gegen Leib und Leben. Im Rahmen von Einflussnahme-Aktivitäten sind viele Staaten bestrebt, auf die politische und öffentliche Meinung in Deutschland im Sinne ihrer langfristigen Ziele einzuwirken.

Daneben stellt die Proliferationsabwehr ein dynamisches Aufgabenfeld dar, welches von politischen, wirtschaftlichen und technischen Entwicklungen geprägt ist. Als High-Tech-Standort ist Deutschland ein bevorzugtes Ziel proliferationsrelevanter Beschaffungsbemühungen.

3. Erkennt die Bundesregierung einen Zuwachs an nachrichtendienstlicher Tätigkeit ausländischer Staaten in Deutschland, und wenn ja, um welche Staaten handelt es sich?

Auf die Antwort zu Frage 2 wird verwiesen.

Die im Fokus der Spionageabwehr stehenden Hauptakteure sind dem jährlichen Verfassungsschutzbericht zu entnehmen. In den letzten Jahren handelt es sich hierbei regelmäßig um die Nachrichtendienste der Russischen Föderation, der Volksrepublik China, der Islamischen Republik Iran und der Republik Türkei.

4. Wie bewertet die Bundesregierung die Zusammenarbeit von Bund und Ländern im Gemeinsamen Extremismus- und Terrorismusabwehrzentrum zu „Spionage einschließlich proliferationsrelevanter Aspekte“ (GETZ S/P)?

   Welche Rolle spielt das GETZ S/P aus Sicht der Bundesregierung für die bundesweite Spionageabwehr?

Die behördenübergreifende Zusammenarbeit bzw. der gegenseitige Informationsaustausch der Bundes- und Landesbehörden innerhalb des GETZ S/P, sowohl im polizeilichen als auch nachrichtendienstlichen Bereich, stellt aus Sicht der Bundesregierung einen wesentlichen Baustein bei der Bekämpfung von Spionageaktivitäten dar.

Das Format des GETZ S/P wird seit 2014 halbjährlich als Austauschforum genutzt.

Der fortlaufende Informationsaustausch in Angelegenheiten der Spionageabwehr erfolgt darüber hinaus außerhalb formaler Gremien. Sowohl die Bund-Länder-Zusammenarbeit als auch die zwischen Nachrichtendiensten und Polizei/Strafverfolgungsbehörden folgt dabei fest etablierten und bewährten Informationssträngen.

a) Welche Arbeitsgruppen bestehen innerhalb des GETZ S/P, welche Behörde ist jeweils für deren Geschäftsführung verantwortlich, und in welchem Turnus treten die Gruppen zusammen?

Folgende Arbeitsgruppen bestehen innerhalb des GETZ S/P:

- AG Lagebesprechung (Geschäftsführung Bundesamt für Verfassungsschutz (BfV) und Bundeskriminalamt (BKA), Tagungsrhythmus: halbjährlich
- AG Gefährdungsbewertung (Geschäftsführung BKA), Tagungsrhythmus: anlassbezogen
- AG Operativer Informationsaustausch (Geschäftsführung BfV und BKA), Tagungsrhythmus: anlassbezogen
- AG Fallanalyse (Geschäftsführung BKA), Tagungsrhythmus: anlassbezogen
- AG Analyse (Geschäftsführung BfV), Tagungsrhythmus: anlassbezogen
- AG Personenpotenzial (Geschäftsführung BfV und BKA), Tagungsrhythmus: anlassbezogen

b) Wieso wurde der Sitzungsrhythmus betreffend der AG Lagebesprechung des GETZ S/P von vierteljährlich auf halbjährlich geändert (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/18932, S. 3)?

Welche Rückschlüsse sind daraus hinsichtlich der Bedrohungslage durch Spionage in Deutschland zu ziehen?

Es wird auf den zweiten Teil der Antwort zu Frage 4 verwiesen. Neben den halbjährlich anberaumten Sitzungen der AG Lagebesprechung finden weitere einzelsachverhaltsbezogene Besprechungen, Arbeitstreffen etc. in Zusammenhang mit bestimmten Ermittlungskomplexen statt, um den dort erforderlichen Informationsaustausch betroffener Behörden, auch mit Blick auf das zugrundeliegende Geheimhaltungsbedürfnis, zu gewährleisten.

Anhand des Sitzungsrhythmus der AG Lagebesprechung lässt sich keinerlei Rückschluss auf die Bedrohungslage durch Spionage in Deutschland ziehen.

c) Wie oft kamen die einzelnen Arbeitsgruppen des GETZ S/P in den vergangenen fünf Jahren zusammen (bitte nach Jahren und Arbeitsgruppen aufschlüsseln)?

Die Arbeitsgruppen traten in den vergangenen fünf Jahren wie folgt zusammen:

	2015	2016	2017	2018	2019	2020
AG Lagebesprechung	2	1	3	2	2	1
AG Operativer Informationsaustausch	2	5	7	1	1	16
AG Gefährdungsbewertung	0	1	0	0	0	0

d) Welche Staaten standen jeweils im Zusammenhang mit sachverhaltsbezogenen Arbeitsgruppensitzungen des GETZ S/P (bitte nach Arbeitsgruppen und Staaten aufschlüsseln)?

Im Zusammenhang mit den sachverhaltsbezogenen Arbeitsgruppensitzungen werden die Staaten thematisiert, die im Fokus der Spionageabwehr und der Bearbeitung entsprechender Operativfälle stehen. Die Schwerpunkte beim Erkenntnisaustausch zu Sachverhalten lagen sowohl bei den Sitzungen der AG Lagebesprechung (allgemeiner Informationsaustausch) als auch bei der AG Operativer Informationsaustausch (einzelsachverhaltsbezogen) insbesondere bei den Ländern Iran, Russland, Türkei sowie VR China.

5. Wie viele Cyberangriffe wurden in den vergangenen fünf Jahren durch deutsche Behörden festgestellt (bitte nach Jahren aufschlüsseln)?

a) Wie groß ist unter den festgestellten Angriffen jeweils der Anteil von Cyberspionage und Cybersabotage?

b) In wie vielen Fällen konnte der Ursprung der Cyberangriffe ermittelt werden?

In wie vielen Fällen waren ausländische, staatliche Stellen für die Angriffe verantwortlich, und welche Staaten waren in diesen Fällen verantwortlich (bitte entsprechend der Fragestellung aufschlüsseln)?

Die Fragen 5 bis 5b werden im Sachzusammenhang beantwortet.

Cyberangriffe bzw. Sicherheitsvorfälle bei Bundesbehörden werden in der Meldestelle des Bundes nach § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erfasst.

Meldungen über Cyberangriffe oder sonstige sicherheitsrelevante Aktivitäten bei Betreibern Kritischer Infrastrukturen im Sinne des BSI-Gesetzes werden durch die Meldestelle gemäß § 8b BSIG beim BSI erhoben. Daneben betreibt das BSI innerhalb der Allianz für Cyber-Sicherheit eine freiwillige Meldestelle für Sicherheitsvorfälle für Unternehmen, die nicht unter die vorgenannte Meldepflicht fallen.

Auswertungen können den jährlichen Lageberichten entnommen werden, die unter der folgenden Adresse öffentlich zugänglich sind: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html. Die erfassten Meldungen lassen keine Trennung danach zu, ob die Angreifer staatliche Nachrichtendienste sind, da sich die Meldepflicht nicht auf diesen Aspekt bezieht.

Sowohl die Unterscheidung in Cybersabotage und -spionage als auch die Zurechnung von Cyberangriffen zu staatlichen Akteuren ist nur in seltenen Fällen eindeutig. Eine belastbare Beantwortung der Frage ist vor diesem Hintergrund nicht möglich.

6. Hat die Bundesregierung im Zusammenhang mit der Covid-19-Pandemie eine Häufung von Cyberangriffen erkannt?

   Wenn ja, wie groß ist unter den festgestellten Angriffen jeweils der Anteil von Cyberspionage und Cybersabotage?

Die Bundesregierung hat im Zusammenhang mit der Covid-19-Pandemie keine Häufung von Cyberangriffen festgestellt. Dabei legt sie die Definition des Begriffs „Cyberangriff“ aus der Cybersicherheitsstrategie für Deutschland 2016 zugrunde.

Festzustellen war jedoch eine Häufung von versuchten und vollendeten Betrugsdelikten, die elektronische Tatmittel nutzten. Hierzu gehört insbesondere die Zunahme von Phishing-Mails, die das Thema Covid-19 in Bezug nahmen und die Nutzung sogenannter Fake-Domains, um Fördermittel oder Daten von Bezugsberechtigten im Zusammenhang mit den Auswirkungen von Covid-19 unrechtmäßig zu erlangen.

Schadsoftwarekampagnen, wie z. B. Ransomware, hielten auch in der Pandemie an. Unter den Betroffenen finden sich auch in der Pandemie wichtige Einrichtungen wie Krankenhäuser, Hersteller von Medizinprodukten oder Schutzausrüstungen. Ein unmittelbarer Bezug dieser Cyberangriffe, um die Pandemiebekämpfung zu beeinträchtigen, konnte bisher nicht nachgewiesen werden.

7. Welche Rolle nimmt das Nationale Cyber-Abwehrzentrum (Cyber-AZ) bei der Abstimmung von Maßnahmen gegen nachrichtendienstliche Cyberangriffe (beispielsweise zur Cyberspionage und Cybersabotage) ein?

   Wie erfolgt an dieser Stelle die Abgrenzung zur Arbeit des GETZ S/P?

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) dient als Informations- und Koordinierungsplattform der derzeit daran beteiligten Behörden (vgl. Antwort der Bundesregierung zu Frage 11 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/21675). Diese Rolle nimmt es unabhängig von der Urheberschaft des jeweils in Rede stehenden Cyberangriffs wahr.

Das GETZ S/P besitzt einen anderen Teilnehmerkreis und ist in Abgrenzung zum Cyber-AZ für die realweltliche Spionageabwehr einschließlich proliferationsrelevanter Aspekte zuständig.

8. Welche weiteren Institutionen sind in Maßnahmen gegen nachrichtendienstliche Cyberangriffe (beispielsweise zur Cyberspionage und Cybersabotage) eingebunden?

   Welche Behörden sind darin ggf. eingebunden (bitte aufschlüsseln)?

Die Zusammenarbeit mit anderen Behörden erfolgt je nach Einzelfallgestaltung, sofern die rechtlichen Voraussetzungen hierfür vorliegen, und kann daher nicht abschließend und aufgeschlüsselt beantwortet werden. Im Übrigen wird auf die Antwort zu Frage 14, 1. Teilfrage verwiesen.

9. Konnte die Bundesregierung die Zielsetzung „einer verstärkten Einbindung der Länder“ in das Cyber-AZ erreichen (s. die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/7607, S. 5)?

   Welche Maßnahmen hat die Bundesregierung getroffen, um eine verstärkte Einbindung der Länder zu erreichen?

   Welche Landesbehörden sind inzwischen im Cyber-AZ konkret vertreten?

Die Bundesregierung verfolgt nach wie vor das Ziel einer geeigneten Einbindung der Länder in das Cyber-AZ. Die zur konkreten Ausgestaltung im ersten Halbjahr 2020 angedachten Workshops konnten aufgrund der COVID-19-Pandemie noch nicht durchgeführt werden.

Allerdings partizipieren die Länder auch heute schon an der Arbeit des Cyber-AZ. Über die Zentralstellenfunktionen des BKA und BfV sowie den Verwaltungs-CERT-Verbund, dem das BSI angehört, werden bei Bedarf Informationen zwischen Cyber-AZ und den Ländern ausgetauscht.

10. Auf welchen konkreten rechtlichen Grundlagen basieren die Zusammenarbeit und der Informationsaustausch im Cyber-AZ hinsichtlich der beteiligten Bundesbehörden?

    Auf welchen konkreten rechtlichen Grundlagen basieren sie nach Kenntnis der Bundesregierung hinsichtlich der beteiligten Länderbehörden (bitte aufschlüsseln)?

Die Zusammenarbeit und der Informationsaustausch basieren auf den einschlägigen Rechtsgrundlagen der teilnehmenden Behörden. Dabei handelt es sich insbesondere um das Bundesverfassungsschutzgesetz (BVerfSchG), Bundeskriminalamtgesetz (BKAG), Gesetz über den Bundesnachrichtendienst (BNDG), Bundespolizeigesetz (BPolG) und BSIG. Infrage kommen sowohl Aufgabennormen wie beispielsweise § 3 Absatz 1 Nummer 12 bis 15 BSIG als auch spezifische Übermittlungsvorschriften in den jeweiligen Gesetzen. Auf welche Rechtsvorschrift sich die Zusammenarbeit im jeweiligen Einzelfall stützt, ist von den konkreten Gegebenheiten abhängig und kann nicht pauschal beantwortet werden.

11. Welche Erkenntnisse liegen der Bundesregierung gegenwärtig zum Cyberangriff auf die BwFuhrpark Service GmbH vor?

Die IT-Systeme der BwFuhrparkService GmbH wurden mit der Schadsoftware Emotet (Erpressungstrojaner) infiziert.

Umfang und das Muster des Hacker-Angriffs lassen darauf schließen, dass es sich hierbei um die Vorbereitung einer Erpressung gegen die BwFuhrparkService GmbH handelt.

Am 13. August 2020 hat die Gesellschaft nach einer detaillierten Erstanalyse vorsorglich ihre IT-Systeme vollständig vom Internet getrennt, um eine weitere Ausbreitung auf andere IT-Systeme sowie weitere Institutionen zu vermeiden. Weder sind Daten auf den IT-Systemen der BwFuhrparkService GmbH verschlüsselt worden, noch sind derzeit erpresserische Handlungen zu Lasten der BwFuhrparkService GmbH bekannt.

a) Wann, wie, und durch welche Stelle wurde der Cyberangriff aufgedeckt?

Der Zugriff auf das IT-System der BwFuhrparkService GmbH wurde am 13. August 2020 durch den IT Security Manager der BwFuhrparkService GmbH festgestellt. Dem vorausgegangen waren diverse Virenmeldungen einschließlich deren Überprüfung und daraus resultierender Gegenmaßnahmen.

b) Welche staatlichen Stellen sind in die Aufklärung des Cyberangriffs eingebunden?

Derzeit ist das Cyber Response Emergency Team des Cyber Security Operations Centre der Bundeswehr, das BKA sowie das BSI in die Aufklärung eingebunden.

In der Informations- und Koordinierungsplattform Cyber-AZ erfolgt im Rahmen der gesetzlichen Grundlagen der teilnehmenden Behörden ein regelmäßiger Informationsaustausch. Die Staatsanwaltschaft Köln hat ebenfalls Ermittlungen aufgenommen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wurde in Kenntnis gesetzt.

c) Konnte der Ursprung des Angriffs ermittelt bzw. auf einen konkreten Urheber zurückgeführt werden?

Trotz intensiver und umfangreicher forensischer Arbeiten konnten Ursprung oder Urheber des Angriffs bislang nicht ermittelt werden. Die Untersuchungen dauern an.

d) In welchem Umfang sind Daten abgeflossen?

Welche Art von Daten sind abgeflossen?

Es gibt bislang keine Erkenntnisse darüber, dass Daten abgeflossen sind.

e) Welche Stellen bzw. Arbeitsebenen waren im Vorfeld des Cyberangriffs für die Systeminfrastruktur der BwFuhrpark Service GmbH bzw. deren Schutz verantwortlich?

Die Verantwortung für die Systeminfrastruktur und deren Schutz obliegt der BwFuhrparkService GmbH.

f) War das Zentrum für Cybersicherheit der Bundeswehr im Vorfeld des Cyberangriffs in den Schutz der Systeminfrastruktur der BwFuhrpark Service GmbH eingebunden?

Wenn ja, in welcher Form?

Wenn nein, wieso nicht?

Nein, da die BwFuhrparkService GmbH nicht in den Zuständigkeitsbereich des Zentrums für Cyber-Sicherheit der Bundeswehr fällt.

g) War das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Vorfeld des Cyberangriffs in den Schutz der Systeminfrastruktur der BwFuhrpark Service GmbH eingebunden?

Wenn ja, in welcher Form?

Wenn nein, wieso nicht?

Das BSI hat das Sicherheitskonzept DSWfahr der BwFuhrparkService GmbH geprüft. Nicht Bestandteil der Prüfung waren: die Backend-Anwendungen von DSW einschließlich des Webservers, die Backend-Systeme von DSW, die Lokationen der Backend-Systeme von DSW, die Schnittstelle zu DSW/DSW-FD und der AuthService. Im Übrigen war das BSI im Vorfeld nicht eingebunden, da das IT-System der BwFuhrparkService GmbH in seiner Gesamtheit nicht in dessen Zuständigkeitsbereich fällt.

12. Wie viele Ermittlungsverfahren zum Bereich von Landesverrat und Gefährdung der äußeren Sicherheit (§§ 93–101a des Strafgesetzbuchs (StGB)) hat der Generalbundesanwalt (GBA) in den vergangenen fünf Jahren geführt?

In wie vielen der Verfahren kam es zu einer Verurteilung (bitte aufschlüsseln)?

Der Generalbundesanwalt beim Bundesgerichtshof hat in den Jahren 2015 bis 2020 bislang insgesamt 98 Ermittlungsverfahren wegen des Verdachts von Straftaten des zweiten Abschnitts des Strafgesetzbuchs (StGB – Landesverrat und Gefährdung der äußeren Sicherheit) eingeleitet. In neun Verfahren kam es gegen zwölf Angeklagte zu rechtskräftigen Verurteilungen. Sieben Angeklagte wurden wegen geheimdienstlicher Agententätigkeit nach § 99 StGB und ein Angeklagter wegen Beihilfe zur geheimdienstlichen Agententätigkeit verurteilt, gegen zwei Angeklagte wurden Urteile wegen Offenbarens von Staatsgeheimnissen nach § 95 StGB verhängt und in einem weiteren gegen zwei Angeklagte gerichteten Verfahren kam es zu einer Verurteilung wegen Landesverrats sowie wegen Beihilfe zum Landesverrat.

13. Wie viele der Verfahren hatten einen Zusammenhang mit einer nachrichtendienstlichen Tätigkeit der Russischen Föderation, der Volksrepublik China, der Republik Türkei, der Arabischen Republik Ägypten sowie der Sozialistischen Republik Vietnam?

Auskünfte zu den in der Frage genannten Staaten können nicht erteilt werden. Trotz der grundsätzlichen verfassungsrechtlichen Pflicht der Bundesregierung, Informationsansprüche des Deutschen Bundestages zu erfüllen, tritt hier nach Abwägung der betroffenen Belange das Informationsinteresse des Parlaments hinter den berechtigten Geheimhaltungsinteressen zurück, da diese Informationen Rückschlüsse auf zum Teil noch verdeckt geführte Ermittlungsverfahren zuließen und damit Ermittlungen beeinträchtigen könnten. Das verfassungs-

rechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird insoweit durch das gleichfalls Verfassungsrang genießende schutzwürdige Interesse an der Gewährleistung einer funktionstüchtigen Strafrechtspflege begrenzt.

14. Welche Maßnahmen ergreift die Bundesregierung, um ausländische Spionageaktivitäten in Deutschland wirkungsvoll zu unterbinden?

Welche gesetzgeberischen Maßnahmen hat sie bereits ergriffen, und welche zukünftigen Maßnahmen plant sie?

Die wesentlichen Bausteine bei der Bekämpfung ausländischer (Cyber-)Spionageaktivitäten stellen der gegenseitige Informationsaustausch der jeweils zuständigen Bundes- und Landesbehörden sowohl im polizeilichen als auch nachrichtendienstlichen Bereich sowie eine konsequente Strafverfolgung dar. Sofern erforderlich werden internationale Partner in die Zusammenarbeit einbezogen. Ein weiterer wesentlicher Baustein ist die Präventionsarbeit durch Vorträge, Veröffentlichungen und Gespräche, insbesondere mit denjenigen Personen aus den Bereichen Wissenschaft, Wirtschaft, Politik und Verwaltung, die im besonderen Fokus fremder Nachrichtendienste stehen, um ausländische Spionageaktivitäten in Deutschland zu unterbinden. Darüber hinaus werden sowohl anlassunabhängige als auch generelle Sensibilisierungsmaßnahmen für Behörden, Wirtschaft und Forschung im Bereich Cybersicherheit im Rahmen des Präventionsauftrags durchgeführt. Dabei werden typische Angriffsmethoden und mögliche Abwehrmaßnahmen erläutert. Im Übrigen wird auf die Antwort zu Frage 16 verwiesen.

Die Bundesregierung betrachtet die Bekämpfung der ausländischen Spionageaktivitäten als wichtiges Handlungsfeld.

Bei der Gewährleistung der Sicherheit der Bundesrepublik Deutschland verfolgt die Bundesregierung jedoch einen ganzheitlichen Ansatz mit der Folge, dass gesetzgeberische Maßnahmen nicht nur verengt auf den Bereich der Spionageabwehr durchgeführt werden, sondern vielmehr einen umfassenden Schutz sicherstellen sollen.

Ein hoher Standard im Bereich der Cyber-und Informationssicherheit stellt einen besonders wirksamen Schutz vor staatlich gesteuerten Cyber-Angriffen dar. Die von der Bundesregierung getroffenen Maßnahmen in diesem Bereich sind vielfältig. Hervorzuheben wären u. a. die Einführung von Mindeststandards für die IT-Sicherheit und Meldepflichten für Betreiber kritischer Infrastrukturen, der Ausbau der Cyber-Fähigkeiten bei den Bundessicherheitsbehörden und des BSI und das IT-Sicherheitsgesetz von 2015, das derzeit unter dem Namen IT-Sicherheitsgesetz 2.0 novelliert wird.

15. Wie viele ausländische Staatsbürger wurden nach Kenntnis der Bundesregierung in den vergangenen fünf Jahren aufgrund nachrichtendienstlicher Tätigkeit aus Deutschland ausgewiesen (bitte nach Jahren und Nationalität aufschlüsseln)?

Aufenthaltsbeendende Maßnahmen gegenüber in Deutschland lebenden Ausländern, wie etwa Ausweisungen gemäß den §§ 53, 54 des Aufenthaltsgesetzes, unterliegen nicht der Zuständigkeit des Bundes; sie sind Ländersache. Eine Statistik zu Ausweisungsgründen wird im Bund nicht geführt. Vor diesem Hintergrund kann eine Auskunft speziell zu etwaigen aufenthaltsbeendenden Maßnahmen gegen Ausländer wegen des Verdachts der geheimdienstlichen Agententätigkeit nicht getroffen werden.

Aufenthaltsbeendende Maßnahmen nach dem Aufenthaltsgesetz sind gegen in Deutschland akkreditierte Diplomaten nicht möglich. Gegen diesen Personenkreis kommen nur Notifizierungen als „persona non grata“ nach Artikel 9 des Wiener Übereinkommens über die Diplomatischen Beziehungen (WÜD) bzw. Artikel 23 des Wiener Übereinkommens über die konsularischen Beziehungen (WÜK) in Betracht.

In den letzten fünf Jahren hat das Auswärtige Amt insgesamt sechs Angehörige der Botschaft der Russischen Föderation und zwei Angehörige der Botschaft der Sozialistischen Republik Vietnam zu „personae non gratae“ erklärt sowie zur Ausreise aufgefordert.

16. Zu welchen Themen wurden in den vergangenen fünf Jahren sog. Sicherheitshinweise durch das Bundesamt für Verfassungsschutz herausgegeben (bitte nach Jahren, Themen und ggf. Anzahl aufschlüsseln)?

Das BfV hat Sicherheitshinweise zu den folgenden Themen herausgegeben:

1. Am 20.05.2020 informierte das BfV darüber, dass neben Gefahren von Cyberattacken auch verstärkte Aktivitäten fremder Nachrichtendienste im Bereich solcher Unternehmen und wissenschaftlicher Einrichtungen zu befürchten sind, die an Impfstoffen, Medikamenten, Antikörpertests und weiteren Innovationen forschen, welche im unmittelbaren Bezug zur Pandemie stehen.
2. Mit Schreiben vom 10. Juni 2020 richtete das BfV einen Sicherheitshinweis an Unternehmen der maritimen Wirtschaft, in welchem es um Vulnerabilitäten moderner Navigationssysteme durch mögliche nachrichtendienstliche Beeinträchtigungen, insbesondere im Zusammenhang mit der Kombination von GPS-Navigation, Radar, AIS (Automatisches Identifikationssystem), elektronische Seekarten etc. in einem einzigen sog. ECDIS (electronic chart display and information system) geht.
3. Im August 2020 hat das BfV gemeinsam mit dem BKA einen Sicherheitshinweis zu Cyberspionage mittels der Schadsoftware GOLDENSPY herausgegeben.

Daneben wird seit Oktober 2015 mehrfach jährlich der „BfV Cyber-Brief“ mit Hinweisen und Informationen zu aktuellen Angriffskampagnen veröffentlicht. Die Themen und Inhalte des Cyber-Briefs und anderer Sicherheitshinweise sind auf der Internetseite des BfV öffentlich einsehbar und nach Monat und Jahr sortiert.

Weiterhin informierte und sensibilisierte das BfV in den letzten Jahren im Rahmen verschiedener Formate die Öffentlichkeit über hier vorliegende Erkenntnisse zu Aktivitäten fremder Nachrichtendienste in Deutschland.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333