

Kleine Anfrage

der Abgeordneten Benjamin Strasser, Stephan Thomae, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Reginald Hanke, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Marcel Klinge, Pascal Kober, Oliver Luksic, Alexander Müller, Frank Müller-Rosentritt, Bernd Reuther, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Dr. Hermann Otto Solms, Dr. Marie-Agnes Strack-Zimmermann, Linda Teuteberg, Gerald Ullrich und der Fraktion der FDP

Spionage in Deutschland

Die Bundesrepublik Deutschland steht im Fokus des Interesses ausländischer Regierung 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-entfuhrung-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 sog. „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 Bundesre-

publik 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 „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 zugeordnet 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>).

Wir fragen die Bundesregierung:

1. Wie schätzt die Bundesregierung die aktuelle Bedrohungslage durch Spionage sowie die Schwerpunkte ausländischer Spionageaktivitäten in Deutschland ein?
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?
3. Erkennt die Bundesregierung einen Zuwachs an nachrichtendienstlicher Tätigkeit ausländischer Staaten in Deutschland und wenn ja, um welche Staaten handelt es sich?
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?

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

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

- c) Wie oft kamen die einzelnen Arbeitsgruppen des GETZ S/P in den vergangenen fünf Jahren zusammen (bitte aufschlüsseln nach Jahren und Arbeitsgruppen)?
- d) Welche Staaten standen jeweils im Zusammenhang mit sachverhaltsbezogenen Arbeitsgruppensitzungen des GETZ S/P (bitte aufschlüsseln nach Arbeitsgruppen und Staaten)?
5. Wie viele Cyberangriffe wurden in den vergangenen fünf Jahren durch deutsche Behörden festgestellt (bitte aufschlüsseln nach Jahren)?
- 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)?
6. Hat die Bundesregierung in 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?
7. Welche Rolle nimmt das Nationale Cyber-Abwehrzentrum (Cyber-AZ) bei der Abstimmung von Maßnahmen gegen nachrichtendienstliche Cyberangriffe (beispielsweise zur Cyberspionage und Cybersabotage)?
- Wie erfolgt an dieser Stelle die Abgrenzung zur Arbeit des GETZ S/P?
8. Welche weitere Institutionen sind in Maßnahmen gegen nachrichtendienstliche Cyberangriffe (beispielsweise zur Cyberspionage und Cybersabotage) eingebunden?
- Welche Behörden sind darin ggf. eingebunden (bitte aufschlüsseln)?
9. Konnte die Bundesregierung die Zielsetzung „einer verstärkten Einbindung der Länder“ in das Cyber-AZ erreichen (s. Bundestagsdrucksache Drucksache 19/7607, S. 5)?
- Welche Maßnahmen hat die Bundesregierung um eine verstärkte Einbindung der Länder zu erreichen?
- Welche Landesbehörden sind inzwischen im Cyber-AZ konkret vertreten?
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)?
11. Welche Erkenntnisse liegen der Bundesregierung gegenwärtig zum Cyberangriff auf die BwFuhrpark Service GmbH vor?
- a) Wann, wie und durch welche Stelle wurde der Cyberangriff aufgedeckt?
- b) Welche staatlichen Stellen sind in die Aufklärung des Cyberangriffs eingebunden?
- c) Konnte der Ursprung des Angriffs ermittelt bzw. auf einen konkreten Urheber zurückgeführt werden?

- d) In welchem Umfang sind Daten abgeflossen?
Welche Art von Daten sind abgeflossen?
- e) Welche Stellen bzw. Arbeitsebenen waren im Vorfeld des Cyberangriffs für die Systeminfrastruktur der BwFuhrpark Service GmbH bzw. deren Schutz verantwortlich?
- f) War das Zentrum für Cyber-Sicherheit 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?
- 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?
12. Wie viele Ermittlungsverfahren zum Bereich von Landesverrat und Gefährdung der äußeren Sicherheit (§§ 93 – 101a StGB) hat der Generalbundesanwalt (GBA) in den vergangenen fünf Jahren geführt?
In wie vielen der Verfahren kam es zu einer Verurteilung (bitte aufschlüsseln)?
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?
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?
15. Wie viele ausländische Staatsbürger wurden nach Kenntnis der Bundesregierung in den vergangenen fünf Jahren aufgrund nachrichtendienstlicher Tätigkeit aus Deutschland ausgewiesen (bitte aufschlüsseln nach Jahren und Nationalität)?
16. Zu welchen Themen wurden in den vergangenen fünf Jahren sog. Sicherheitshinweise durch das Bundesamt für Verfassungsschutz (BfV) herausgegeben (bitte aufschlüsseln nach Jahren, Themen und ggf. Anzahl)?

Berlin, den 26. August 2020

Christian Lindner und Fraktion