Deutscher Bundestag **Drucksache 20/14595**

20. Wahlperiode 21.01.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Renata Alt, Christine Aschenberg-Dugnus, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 20/14166 –

Hybride Angriffe und Desinformation im Vorfeld der Bundestagswahl

Vorbemerkung der Fragesteller

In Zeiten zunehmender internationaler Spannungen sind hybride Angriffe und Desinformation für autoritäre Staaten ein Mittel, um Druck auf demokratische Staaten auszuüben und gezielt auf die öffentlichen Debatten in liberalen Demokratien Einfluss zu nehmen. Die verwendeten Mittel reichen hierbei von Desinformation auf Social Media (vgl. www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt, letzter Abruf: 25. November 2024) über Sabotage an kritischer Infrastruktur (vgl. www.zdf.de/nachrichten/politik/ausland/ostsee-finnland-schweden-litauen-unterseekabel-100.html, letzter Abruf 25. November 2024) bis zu Spionage (vgl. www.tagesschau.de/investigativ/ndr-wdr/drohnen-spionage-sabotage-100.html, letzter Abruf: 25. November 2024). Ausländische Staaten nehmen auch ganz direkt Einfluss auf die politische Willensbildung, indem sie beispielsweise deutsche Politiker oder deren Mitarbeiter anwerben (vgl. www.tagesschau.de/investigativ/wdr/spionage-china-deutschland-100.html, letzter Abruf 25. November 2024) oder anderweitig in die politische Willensbildung in Deutschland eingreifen. Auch ausländisch beeinflusste Institutionen dienen dabei immer häufiger als Eintrittstor für fremde Mächte (vgl. www.deutschlandfunk.de/ditib-ankaras-einfluss-auf-deutschen-moscheeverband-100.html, letzter Abruf 25. November 2024). Zunehmend setzt sich das Konzept der „Foreign Information Manipulation and Interference“ (FIMI) durch und meint gezielte Aktivitäten ausländischer Akteure, die darauf abzielen, durch Manipulation und gezielte Desinformation das öffentliche Meinungsbild, demokratische Prozesse oder die gesellschaftliche Stabilität in anderen Staaten zu beeinflussen (vgl. www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en; letzter Abruf: 28. November 2024). Die Gefahr hybrider Einflussnahme besteht insbesondere mit Blick auf die vorgezogene Bundestagswahl am 23. Februar 2025 (vgl. www.tagesspiegel.de/politik/naturlich-hat-das-auswirkungen-bnd-chef-kahl-warnt-vor-einflussversuchen-moskaus-auf-bundestagswahl-12782207.html; letzter Abruf: 28.11.2024).

Die Bundesrepublik Deutschland ist insbesondere für die hybriden Aktivitäten der Russischen Föderation ein wichtiges und gleichzeitig leichtes Ziel. Das Parlamentarische Kontrollgremium (PKGr) des Deutschen Bundestages hat in seiner Öffentlichen Bewertung vom 13. März 2024 festgestellt, dass Deutsch-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 21. Januar 2025 übermittelt.

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

land im Mittelpunkt russischer Einflussoperationen steht. Russland versuche aktiv und erfolgreich, auf verschiedenen Ebenen illegitim auf Politik, Wirtschaft und Gesellschaft einzuwirken. Dabei werde die Tragweite der Bedrohung weder von allen politisch Verantwortlichen noch in der Gesellschaft in Deutschland insgesamt erkannt. Der Instrumentenkasten hybrider Angriffe reicht von umfangreichen Desinformationskampagnen in Medien, sozialen Netzwerken und auf Plattformen, massiver Propaganda über Hack- and Leak-Operationen, Spionage und Cyberangriffe, gezielte Instrumentalisierung und Förderung von Migration, Wahlbeeinflussung und Beeinflussung der politischen Willensbildung bis hin zur – auch finanziellen – Unterstützung extremistischer Gruppierungen. Ziele der Angriffe seien Destabilisierung, Verunsicherung und gesellschaftliche Spaltung (vgl. Öffentliche Bewertung des Parlamentarischen Kontrollgremiums gemäß § 10 Absatz 2 Satz 1 des Kontrollgremiumgesetzes vom 13. März 2024 – Russische Einflussnahme in Deutschland, Bundestagsdrucksache 20/10655).

Anders als FIMI und Desinformationen, die ihre Wirkung oft erst schleichend entfalten und sich erst im Laufe der Zeit materialisieren, führen hybride Angriffe auch zu ganz konkreten und unmittelbaren Schäden in Deutschland. Deutsche Unternehmen und staatliche Einrichtungen sind konstant Ziel von Cyberattacken. Alleine der Schaden für die deutsche Wirtschaft betrug 2023 einen dreistelligen Milliardenbetrag (www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2024/2024-08-28-studie-bitkom.html#:~:text=Aktuell%20sind%20Cyberattacken%20f%C3%BCr,betrug%20der%20Schaden%20durch%20Cybercrime., letzter Abruf 25. November 2024). Daneben kommt es aber immer häufiger auch zu Sabotage, Spionage und ganz konkreten Angriffen auf kritische Infrastruktur, sei es bei Seekabeln oder im Logistikbereich. Die Dreistigkeit der Täter wächst, während es den deutschen Sicherheitsbehörden schwerfällt, die Täter dingfest zu machen. So waren es beispielsweise dänische Marineschiffe, die einen chinesischen Frachter festsetzten, der im großen Umfang Unterseekabel beschädigt hatte, während die deutsche Bundespolizei erst verspätet ausrückte (vgl. www.ndr.de/nachrichten/mecklenburg-vorpommern/Moegliche-Kabel-Sabotage-in-Ostsee-Bundespolizei-schickt-Schiff,kabelsabotage100.html, letzter Abruf 25. November 2024).

Vorbemerkung der Bundesregierung

Nach Verständnis der Bundesregierung bezeichnet der Begriff „Hybrider Angriff“ das gegnerische Agieren anderer Staaten unterhalb der Schwelle eines direkten Angriffs. Die jeweiligen Angriffsformen stellen die Instrumente hybrider Bedrohungen dar und können verschleiert erfolgen, um eine unmittelbare Zuordnung zu erschweren. Hybride Bedrohungen können daher vielfältige Formen, wie Sabotageakte, gezielte Desinformation, Cyberangriffe, Anschläge und Attentate, aber auch den Einsatz konventioneller militärischer Mittel annehmen. Die Bundesregierung macht sich die Einschätzungen der Fragenstellerinnen und Fragensteller nicht zu eigen.

Darüber hinaus ist darauf hingewiesen, dass anders als in der Vorbemerkung der Fragestellerinnen und Fragensteller dargestellt unmittelbar nach Kenntnis von der Beschädigung des Unterseekabels C-Lion 1 zwei Einsatzschiffe der Bundespolizei entsandt wurden, um die Schadenstelle zu dokumentieren und den Frachter YI PENG 3 im Kattegat zu überwachen.

1. Wie erfasst die Bundesregierung hybride Angriffe auf Deutschland oder deutsche Infrastruktur, und welche Kriterien legt die Bundesregierung bei dieser Erfassung zugrunde?

2. Wie viele hybride Angriffe auf Deutschland oder deutsche Infrastruktur hat die Bundesregierung seit dem Jahr 2010 jeweils jährlich festgestellt, welche Entwicklungen sind bei diesen Zahlen aus Sicht der Bundesregierung zu beobachten, und wie erklärt sich die Bundesregierung einen eventuellen Anstieg hybrider Angriffe in den letzten Jahren?

3. Welche Akteure führen hybride Angriffe auf Deutschland oder deutsche Infrastruktur aus, wie stellt die Bundesregierung diese Akteure fest, welche Konzepte zur Identifizierung von Urhebern solcher Angriffe hat die Bundesregierung entwickelt, und wie wendet sie diese an?

Die Fragen 1 bis 3 werden gemeinsam beantwortet.

Die Bundesregierung führt keine Statistiken bezüglich hybrider Bedrohungen gegen Deutschland oder deutsche Infrastruktur gerichtete hybride Aktivitäten. Aktuelle Fälle werden im laufenden Austausch unter den zuständigen Ressorts und Stellen in der wöchentlich stattfindenden Task Force gegen Desinformation und weitere hybride Bedrohungen besprochen.

Es wird zudem auf die Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/12872 verwiesen.

Die Fälle werden anhand der individuellen Ausprägungen einer möglichen hybriden Bedrohung phänomenologisch den zuständigen Stellen zugeordnet. Zudem besteht ein Austausch der Bundesregierung mit ausländischen Partnern, auch in der EU und in der NATO, welcher zu einem besseren Lageverständnis zur hybriden Bedrohungslage beiträgt. Bezüglich der Akteure, die hybride Angriffe auf Deutschland oder deutsche Infrastruktur führen, wird auf die jährlichen Verfassungsschutzberichte verwiesen.

4. Welcher Schaden entsteht nach Kenntnis der Bundesregierung durch hybride Angriffe jährlich in Deutschland (bitte jährlich seit 2010 aufschlüsseln), und wie erklärt sich die Bundesregierung die Kostenentwicklung dieser Angriffe?

5. Welche Schadensereignisse stechen aus Sicht der Bundesregierung durch ihre besonders hohen Kosten insoweit heraus?

Die Fragen 4 und 5 werden gemeinsam beantwortet.

Die Bundesregierung führt keine Statistiken über die Kosten, die durch hybride Bedrohungen verursacht werden.

6. Wie viele Cyberangriffe auf deutsche Unternehmen, staatliche Einrichtungen und Infrastruktur hat es seit 2021 jeweils jährlich gegeben, welche Schäden haben diese Angriffe jeweils jährlich verursacht, und welchen Anteil haben dabei die Angriffe staatlicher Akteure nach Kenntnis der Bundesregierung?

Die Bundesregierung führt keine entsprechenden umfassenden Statistiken zur Beantwortung dieser Fragen. Mit Bezug zu einzelnen Phänomen- bzw. Bezugsbereichen können die folgenden Angaben gemacht werden:

Die Bundesregierung geht davon aus, dass mit der Frage nach Cyberangriffen auf die „staatliche […] Infrastruktur“ die „Kritische Infrastruktur“ („KRITIS“) gemeint ist. Im Bereich der Kritischen Infrastruktur erfasst das Bundesamt für Sicherheit in der Informationstechnik (BSI) Meldungen von KRITIS-Betreibern über Cybersicherheitsvorfälle. Die KRITIS-Betreiber sind gemäß § 8b Absatz 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) verpflichtet, dort näher bestimmte Cybersicherheitsvorfälle unverzüglich dem BSI zu melden.

Seit 2021 hat es folgende Meldungen von KRITIS-Betreibern zu Cybersicherheitsvorfällen gemäß § 8b Absatz 4 BSIG gegeben:

2021	**2022**	**2023**	**2024**
385	475	537	769

Es ist bei den Meldungen zu berücksichtigen, dass nicht hinter jeder Vorfallsmeldung notwendigerweise ein Cyberangriff steht. Nicht in jedem Fall ließ sich abschließend durch den Betreiber aufklären, ob dem Cybersicherheitsvorfall ein Angriff oder eine andersartige Ursache zu Grunde lag. Entsprechend ist auch unbekannt, welchen Anteil etwaige staatliche Akteure an den Cybersicherheitsvorfällen bei KRITIS-Betreibern tragen.

Die in der polizeilichen Kriminalstatistik (PKS) erfassten Straftaten im Bereich Cybercrime, welche sich generell auf Geschädigte in Deutschland beziehen, lagen für das Jahr 2021 bei 146 363, 2022 bei 136 865 und 2023 bei 134 407. Dabei ist zu berücksichtigen, dass in diesen Zahlen diejenigen Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters/der Täterin bzw. der Täter im Ausland liegt oder unbekannt ist (sogenannte „Auslandstaten“), nicht berücksichtigt sind.

Die Auslandstaten im Bereich Cybercrime werden im Rahmen der PKS seit 2020 erfasst. Nach gemeinsamer Evaluation und Abstimmung mit den Bundesländern ist eine erstmalige Ausweisung der absoluten Zahlen der Straftaten im Bereich Cybercrime zum Berichtsjahr 2024 vorgesehen. Zum aktuellen Zeitpunkt kann lediglich die prozentuale Steigerung seit 2020 angegeben werden. Im Jahr 2021 wurde eine Steigerung der Auslandstaten bei Cybercrime um 34 Prozent festgestellt, 2022 um acht Prozent und 2023 um 28 Prozent. Als Größenreferenz gilt, dass die Auslandstaten bei Cybercrime in den Jahren 2022 und 2023 die der Inlandstaten überstiegen.

Gemäß einer für das Jahr 2023 beim Bundeskriminalamt und den Landeskriminalämtern durchgeführten Fallerhebung haben bundesweit über 800 Unternehmen und Institutionen Ransomware-Fälle zur Anzeige gebracht. Für die vorherigen Jahre liegen der Bundesregierung keine vergleichbaren Statistiken vor.

Zu Fallzahlen anderer Cyber-Angriffsarten können seitens der Bundesregierung mangels entsprechender Statistiken keine Aussagen getroffen werden.

Die oben genannten Erhebungen im Rahmen der PKS beleuchten ausschließlich das polizeiliche Hellfeld, also die polizeilich bekannt gewordene Kriminalität. Im Bereich der Cyberkriminalität ist das Dunkelfeld im Vergleich zu anderen Phänomenbereichen überdurchschnittlich ausgeprägt. Eine Studie des Kriminologischen Forschungsinstituts Niedersachsen e. V. (KFN) schätzte dieses Dunkelfeld zuletzt auf bis zu 91,5 Prozent.

Anhand der geführten polizeilichen Statistiken und der dem BSI von den KRITIS-Betreibern gemeldeten Daten zu Cybersicherheitsvorfällen können keine belastbaren Aussagen zu Schäden, die Cyberangriffe verursachten, getroffen werden.

Eine differenzierte Aussage zum Anteil der Cyberangriffe durch staatliche Akteure in Bezug auf die oben gemachten Angaben zu Cyberangriffen und Straftaten im Bereich Cybercrime ist auf Grundlage der seitens der Bundesregierung geführten Statistiken nicht möglich.

In Bezug auf den Fragegegenstand Cyberangriffe auf staatliche Einrichtungen kann eine Beantwortung durch die Bundesregierung nicht offen erfolgen. Die darin enthaltenen Informationen zu IT-Sicherheitsvorfällen im Zusammenhang mit Cyberangriffen auf deutsche Bundesbehörden sind schützenswert, weil sie potenziellen Angreifern (staatlichen oder nichtstaatlichen Akteuren) eine Einschätzung über die IT-Sicherheitslage der deutschen Bundesbehörden ermöglichen würden oder zumindest geeignet wären, mit weiteren Informationen eine solche Einschätzung zu erlangen. Es handelt sich daher um Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können. Daher ist der entsprechende Antwortteil als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS-Nur für den Dienstgebrauch“ eingestuft.*

7. Wie plant die Bundesregierung, hybriden Angriffen mit Bezug zur Bundestagswahl zu begegnen?

Zum Schutz der Bundestagswahl 2025 vor hybriden Bedrohungen führen die zuständigen Behörden im Rahmen ihrer fachlichen Zuständigkeiten und nach Maßgabe der gesetzlichen Befugnisse eine Vielzahl an Maßnahmen der Prävention, Detektion und Reaktion durch.

8. Sieht die Bundesregierung Bedarf an einem Lagebild zur hybriden Gefährdungslage Deutschlands, und auf welche Art und Weise unterrichtet die Bundesregierung die Bevölkerung, Länder und Kommunen sowie Unternehmen über mögliche Gefährdungen und die richtige Verhaltensweise zum Schutz vor hybriden Angriffen?

Die Bundesregierung prüft laufend und in Abhängigkeit eines Ereignisses geeignete Berichtsformen und stellt mehrsprachig umfangreiche Informationsmaterialien zur Sensibilisierung der Öffentlichkeit für das Thema „Desinformation als hybride Bedrohung“ und spezifisch zum Thema „Schutz der Bundestagswahl 2025 vor hybriden Bedrohungen einschließlich Desinformation“ bereit. Diese sind auf der Internetseite des Bundesministeriums des Innern und für Heimat (BMI) veröffentlicht und unter diesen Links abrufbar: www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html sowie www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation-bei-bt-wahl/desinfo-bei-bt-wahl-artikel.html.

Die Länder und ihre Kommunen werden über die Bund-Länder-offene Arbeitsgruppe Hybride Bedrohungen (BLoAG Hybrid) in der Struktur der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) sowie über den Verfassungsschutzverbund über Gefährdungslagen und Verhaltensweisen zum Schutz vor hybriden Bedrohungen unterrichtet. Die BLoAG Hybrid hat Empfehlungen zur Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation erarbeitet. Sie sind auf der Internetseite des BMI veröffentlicht und unter diesem Link abrufbar: www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/heimat-integration/wehrhafte-demokratie/BMI24013.html.

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

9. Bei wie vielen und welchen untergesetzlichen Normen sieht die Bundesregierung Anpassungsbedarf im Rahmen der Nationalen Sicherheitsstrategie, und inwieweit wurden Punkte der Nationalen Sicherheitsstrategie in Bezug auf hybride Angriffe bereits umgesetzt?

Die Maßnahmen zur Verbesserung der Resilienz gegenüber hybriden Bedrohungen, die in der Nationalen Sicherheitsstrategie aufgeführt sind, ergeben sich u. a. aus dem Kapitel „Resilient: Die Sicherung unserer Werte durch innere Stärke“ (S. 46 ff. der Nationalen Sicherheitsstrategie). Zudem dienen diverse sicherheitspolitische Maßnahmen auch der Steigerung der Widerstandsfähigkeit gegen hybride Bedrohungen.

Die Bundesregierung nutzt die bestehenden Mechanismen und Strukturen zur besseren Erkennung und Abwehr hybrider Bedrohungen in EU, NATO und G7 und entwickelt diese laufend fort.

10. Wie organisiert die Bundesregierung den Informationsaustausch der verschiedenen beteiligten Behörden bei der Erkennung und Abwehr hybrider Angriffe, welche Behörden stehen hierbei im Austausch, welche Austauschformate gibt es, wie oft findet der Austausch statt, und wie viele Fälle werden hierbei jeweils besprochen?

Es wird auf die Antwort der Bundesregierung zu den Fragen 15 bis 22 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13880 verwiesen.

11. Welche Rolle spielen insoweit die gemeinsamen Zentren des Bundes und der Länder (Gemeinsames Terrorismusabwehrzentrum (GTAZ), Gemeinsames Terrorismus- und Extremismusabwehrzentrum (GETZ), Gemeinsames Internetzentrum (GIZ), Nationales Cyber-Abwehrzentrum (NCAZ) und andere)?

Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) und das Gemeinsame Extremismus und Terrorismusabwehrzentrum (GETZ) sind die Kommunikationsplattform für Polizei und Nachrichtendienste auf Bundes- und Länderebene zur Bekämpfung des Rechts-, Links- und auslandsbezogenen Extremismus und Terrorismus sowie der Spionageabwehr einschließlich proliferationsrelevanter Aspekte.

Im Bereich der Informationssicherheit, insbesondere hinsichtlich Cybersachverhalten mit gesamtstaatlicher Relevanz, besteht ein ständiger und intensiver Austausch zwischen den zuständigen Behörden auf verschiedenen Ebenen. Das Nationale Cyber-Abwehrzentrum, eine Kooperations-, Kommunikations- und Koordinationsplattform von deutschen (Sicherheits-)Behörden und weiteren Einrichtungen unterschiedlicher Ressorts, dient in diesem Zusammenhang als Plattform, auf der die beteiligten Behörden Informationen im Rahmen ihrer jeweiligen gesetzlichen Befugnisse schnell austauschen und gegebenenfalls Schutz-, Gefahrenabwehr- oder Strafverfolgungsmaßnahmen koordinieren können.

12. Welche Maßnahmen hat die Bundesregierung ergriffen, um den illegalen Überflügen mit Drohnen über deutsche Bundeswehrstandorte und die Militäreinrichtungen befreundeter ausländischer Staaten in Deutschland entgegenzuwirken, und welche Maßnahmen hat die Bundesregierung ergriffen, um die Urheber dieser Überflüge zu ermitteln?

Am 15. Januar 2025 hat die Bundesregierung Regelungsvorschläge zur Änderung des Luftsicherheitsgesetzes beschlossen, mit dem die Bundeswehr bei einem drohenden besonders schweren Unglücksfall die Befugnis erhalten soll, illegal fliegende Drohnen abzuwehren. Voraussetzung ist, dass die für die Gefahrenabwehr grundsätzlich zuständigen Polizeien der Länder technisch dazu nicht in der Lage sind und entsprechende Unterstützung anfordern. Der Gesetzentwurf soll durch die Regierungsfraktionen in den Deutschen Bundestag eingebracht werden.

Die Bundeswehr baut ihre vorhandenen Fähigkeiten zur Detektion und Abwehr von unbemannten kleinen Luftfahrzeugen kontinuierlich weiter aus. Die Zusammenarbeit der Bundeswehr mit den weiteren zuständigen Behörden, insbesondere der Länder, wird laufend überprüft und optimiert.

13. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Sicherheit von Transportwegen in Deutschland und von bzw. nach Deutschland zu gewährleisten, welche Gefahr geht aus Sicht der Bundesregierung insoweit von Angriffen auf Transportwege auf dem Land-, Luft- und Seeweg jeweils aus, und welche Arten von Angriffen sind hierbei wahrscheinlich, und wie können diese jeweils verhindert werden?

Weltweite Konflikte und Krisen können sich gefährdungserhöhend auf die Transportwege in Deutschland und von bzw. nach Deutschland auswirken. Mögliche Bedrohungsszenarien reichen von Sabotage über Cyberangriffe auf IT-Systeme bis hin zu Angriffen auf Kritische Infrastrukturen. Insbesondere maritime kritische Infrastrukturen sind dabei von einer grundsätzlich hohen Verletzlichkeit gekennzeichnet.

Im Bereich der Schiene können folgende prioritäre Maßnahmen der Deutschen Bahn AG (DB) exemplarisch genannt werden: Aufbau zusätzlicher Redundanzen, stetiges Durchführen von Risikoanalysen in Abstimmung mit den Sicherheitsbehörden, Intensivierung des Streckenschutzes, Einsatz von Videotechnik an unbesetzten Stellwerken im Rahmen der unternehmerischen Sicherheitsvorsorge sowie Beantragung eines Forschungsprojektes über das Bundesministerium für Bildung und Forschung (BMBF) zur Testierung von Außensensorik an einem Zug in Kombination mit der Infrastruktur zum Erkennen bahnbetriebsgefährdender Unregelmäßigkeiten im und am Fahrweg.

Im Bereich der Luftfahrt wird die Sicherheit des Luftverkehrs maßgeblich durch verbindliche Vorgaben der Europäischen Union gewährleistet, insbesondere durch die Verordnung (EG) Nr. 300/2008 vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt. Diese enthält Vorgaben zum Schutz der Zivilluftfahrt vor unrechtmäßigen Eingriffen und wird ergänzt durch europäische Durchführungsbestimmungen. Mitgliedstaaten haben außerdem die Möglichkeit, aufgrund von Risikobewertungen strengere Maßnahmen zu ergreifen.

Im Logistiksektor stellt das Bundesministerium für Digitales und Verkehr (BMDV) u. a. sicher, dass in Krisensituationen über Risiken und geplante oder ergriffene Gegenmaßnahmen – auch im Falle von Angriffen auf Transportwege – schnell informiert wird.

Im Bereich der Schifffahrt finden zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen die Regelungen der Verordnung (EG) Nr. 725/2004 vom 31. März 2004 des Europäischen Parlaments und des Rates Anwendung.

Die Luft- und Seewege außerhalb des nationalen Hoheitsbereichs bieten mannigfaltige Angriffsmöglichkeiten für ausländische Akteure. Diese reichen von niederschwelligen Sabotageakten, über Cyberangriffe auf IT-Systeme bis hin zur gezielten Zerstörung von kritischen Infrastrukturen. Die Bundesregierung arbeitet eng mit ihren Alliierten und Partnern zusammen, um die Resilienz gegen und Abschreckung von hybriden Bedrohungen – auch außerhalb des eigenen nationalen Hoheitsbereiches – zu erhöhen. Im Rahmen der NATO wurden unter anderem Strukturen und Prozesse zur Verbesserung des Schutzes Kritischer Unterwasser-Infrastruktur aufgestellt.

Die Polizeien von Bund und Ländern treffen nach eigener Lagebeurteilung erforderliche polizeiliche Maßnahmen zur Gefahrenabwehr im Rahmen ihrer jeweiligen Zuständigkeiten.

14. Inwiefern erfasst die Bundesregierung gezielte Desinformation ausländischer staatlicher Akteure in Deutschland oder im deutschsprachigen Internet, welche Kriterien legt die Bundesregierung dieser Erfassung zugrunde, und welche Kriterien legt die Bundesregierung zugrunde, um relevante Fälle von Desinformation zu identifizieren, auf die eine koordinierte Erwiderung erfolgen muss?

15. Wie viele Fälle gezielter Desinformation ausländischer staatlicher Akteure in Deutschland oder im deutschsprachigen Internet hat die Bundesregierung seit dem Jahr 2010 jeweils jährlich festgestellt, welche Entwicklungen sind bei diesen Zahlen aus Sicht der Bundesregierung zu beobachten, und wie erklärt sich die Bundesregierung einen eventuellen Anstieg von Desinformation in den letzten Jahren?

16. Welche ausländischen staatlichen oder staatsnahen Akteure verbreiten Desinformation in Deutschland oder im deutschsprachigen Internet, wie stellt die Bundesregierung diese Akteure fest, welche Konzepte zur Identifizierung von Urhebern solcher Verbreitung hat die Bundesregierung entwickelt, und wie wendet sie diese an?

Die Fragen 14 bis 16 werden gemeinsam beantwortet.

Es wird auf die Antwort der Bundesregierung zu den Fragen 11 bis 19 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/12872 sowie auf die Antwort der Bundesregierung zu den Fragen 6 bis 11 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13880 verwiesen.

17. Wie arbeitet die Bundesregierung mit Betreibern von Social-Media-Plattformen zusammen, um Desinformationskampagnen und hybride Angriffe frühzeitig zu erkennen und effektiv einzudämmen?

Es wird auf die Antwort der Bundesregierung zu den Fragen 1 bis 5 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13880 verwiesen.

Im Vorfeld der Bundestagswahl führt das BMI mit den Betreibern großer sozialer Netzwerke Gespräche zum Schutz der Bundestagswahl vor ausländischer Manipulation und Einflussnahme im Informationsraum.

Das Auswärtige Amt führt anlassbezogen Gespräche mit Vertretern von Plattformen. Im Fokus stehen dabei u. a. die Auswirkungen auf Partnerstaaten, insbesondere kleinere Staaten, deren Sprachen weniger Moderation erfahren.

18. Welcher Schaden entsteht nach Kenntnis der Bundesregierung durch Desinformation jährlich (bitte jährlich seit 2010 aufschlüsseln), welche Kosten verursachen insbesondere Gegenmaßnahmen der Bundesregierung, und wie erklärt sich die Bundesregierung die Kostenentwicklung?

Desinformation stellt eine beträchtliche Gefahr für die Demokratie und die freiheitliche demokratische Grundordnung dar. Desinformation kann die öffentliche Sicherheit und Ordnung erheblich gefährden und den gesellschaftlichen Zusammenhalt schwächen.

Bezüglich der dadurch entstandenen Kosten wird auf die Antwort zu Frage 4 verwiesen.

Im Übrigen verweist die Bundesregierung auf die Antworten zu den Fragen 10 und 11 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/17073.

19. Welche Desinformationsereignisse stechen aus Sicht der Bundesregierung durch ihre besonders weitreichenden Folgen heraus, und wie plant die Bundesregierung, solchen Ereignissen zukünftig zu begegnen?

Es wird auf die Antworten zu den Fragen 27 bis 29 verwiesen.

Desinformation betrifft alle Bereiche der deutschen Außen- und Sicherheitspolitik. Hierzu gehört auch die Destabilisierung von Partnerstaaten. Das Auswärtige Amt hat deshalb in den vergangenen Jahren sowohl die internationale Kooperation als auch die hausinternen Analysekapazitäten ausgebaut. Dabei werden insbesondere auch die Mitarbeitenden an deutschen Auslandsvertretungen in der Erkennung von Desinformation und Methoden der Informationsmanipulation geschult, um global ausländischer Desinformation entgegenzuwirken.

Es wird im Übrigen auf die Antwort zu den Fragen 4 und 5 sowie auf die Antwort der Bundesregierung zu den Fragen 6 bis 11 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13880 verwiesen.

20. Wie viele Versuche, die Verbreitung des Programms der in Deutschland verbotenen Fernsehsender RT und Sputnik hat die Bundesregierung seit dem Verbot festgestellt, und wie geht die Bundesregierung gegen die Verbreitung dieser Inhalte vor?

Beiträge von RT und Sputnik werden auf für diesen Zweck eingerichtete Internetseiten (sogenannte Spiegelseiten) und in Sozialen Medien verbreitet. Private und staatliche Akteure nutzen hierfür eine Vielzahl von Konten auf unterschiedlichen Plattformen. Die so erzeugten Inhalte werden geteilt, und verbreiten sich so im Internet. Eine genaue Bezifferung ist aufgrund dieses komplexen und dezentralen Ansatzes nicht möglich.

Gegenstand der geltenden medienspezifischen EU-Sanktionen ist das Verbot der Verbreitung der Inhalte bestimmter russischer Medienunternehmen wie RT und Sputnik auf allen Verbreitungswegen. Das Verbreitungsverbot wird in Deutschland in weiten Teilen eingehalten. Verstöße gegen das genannte Sende- bzw. Verbreitungsverbot sind nach dem Außenwirtschaftsrecht strafbewehrt

und liegen damit im Zuständigkeitsbereich der Strafverfolgungsbehörden der Länder.

21. Plant die Bundesregierung eine Öffnung für fremdsprachige Inhalte der Deutschen Welle auch in Deutschland, und welche Bedeutung misst die Bundesregierung einem solchen Schritt bei der Bekämpfung von FIMI in Deutschland bei?

Die Deutsche Welle hat einen gesetzlichen Auftrag zur Verbreitung von Rundfunk und Telemedien für das Ausland. Die Bundesregierung plant hieran derzeit keine Änderung.

22. Ist der von Russland hergestellte Impfstoff „Sputnik V“ seit 2020 in Deutschland verimpft worden, und wenn ja, wie viele Dosen dieses Impfstoffs wurden verabreicht, wird dieser Impfstoff weiterhin in Deutschland verwendet, und wenn ja, wo und in welchem Umfang?

Der in Russland entwickelte COVID-19-Impfstoff „Sputnik V“ war in Deutschland weder zugelassen noch verfügbar. Nach Kenntnisstand der Bundesregierung wurde dieser Impfstoff in Deutschland nicht angewendet. Im Übrigen wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Faktion der FDP zu Sputnik V auf Bundestagsdrucksache 19/29495 verwiesen.

23. Wie bewertet die Bundesregierung die Einflussnahme ausländischer Akteure und Regierungen auf deutsche Parteien, hat die Bundesregierung dahin gehend Erkenntnisse, dass eine finanzielle Einflussnahme auf deutsche Parteien oder Politiker im Vorfeld der bevorstehenden Bundestagswahl geplant ist oder bereits durchgeführt wird?

Grundsätzlich versuchen fremde Staaten – auch unter Einsatz nicht-staatlicher Akteure – unter anderem auf politische Entscheidungsprozesse einzuwirken. Hiervor wird regelmäßig gewarnt, so zum Beispiel im jährlich erscheinenden Verfassungsschutzbericht. Bislang liegen keine konkreten Erkenntnisse zu finanziellen Einflussnahmeversuchen ausländischer Akteure auf die Bundestagswahl 2025 vor. Mit hybriden Aktivitäten, die darauf abzielen, die Bevölkerung zu verunsichern und das politische System zu untergraben, ist aber zu rechnen. Hierzu können neben Einflussnahme und Desinformation auch Cyberangriffe und Sabotageaktivitäten zählen. Aktuelle Entwicklungen im Zusammenhang mit der Wahl in Rumänien unterstreichen das Gefährdungspotential.

24. Wie erfasst die Bundesregierung Desinformation, wie bewertet sie diese inhaltlich, und nach welchen Kriterien entscheidet sie, auf welche Desinformation gezielt geantwortet werden muss, wie betreibt die Bundesregierung sogenanntes Debunking, also das Entkräften falscher Informationen, und welche nationalen Stellen des Bundes und der Länder bzw. Kommunen stehen insoweit im Austausch?

Auf die Antwort zu den Fragen 1 bis 3 wird verwiesen.

Die Entscheidung über ein mögliches aktives Debunking erfolgt auf Grundlage einer Analyse der Methodik und Verbreitung der möglichen Desinformation. Hierbei spielt auch die potentielle Wirkung der Desinformation eine wesentliche Rolle.

Grundsätzlich gilt: Je höher das Gefährdungspotential eingestuft wird, desto wichtiger ist es, schnell zu reagieren und entschieden gegenzusteuern. In entsprechenden Fällen kann sich die Bundesregierung für ein sogenanntes Debunking, also das aktive Widerlegen falscher oder irreführender Information, entscheiden.

25. Welche technologischen Innovationen und KI-gestützten Lösungen setzt die Bundesregierung ein, um hybride Angriffe und Desinformation frühzeitig zu erkennen?

Die Bundesregierung prüft laufend die Einsatzmöglichkeiten innovativer technologischer Lösungen im Rahmen der rechtlichen Möglichkeiten und Rahmenbedingungen.

26. Welche Maßnahmen ergreift die Bundesregierung, um zivilgesellschaftliche Organisationen, Wissenschaft und Medien in die Erkennung und Bekämpfung von hybriden Angriffen und Desinformation einzubinden, und welche Kooperationen existieren hierzu?

Auf die Antwort zu Frage 9 wird verwiesen.

Aus Sicht der Bundesregierung ist die Arbeit zivilgesellschaftlicher Organisationen und der Wissenschaft zum Umgang mit hybriden Bedrohungen einschließlich Desinformation von großer Bedeutung. Die Bundesregierung arbeitet im Bereich des Umgangs mit hybriden Bedrohungen einschließlich Desinformation mit zivilgesellschaftlichen Organisationen und der Wissenschaft zusammen. Unter anderem hat das BMI mit der Bertelsmann Stiftung im Projekt „Forum gegen Fakes – Gemeinsam für eine starke Demokratie“ kooperiert, dabei wurden auch weitere zivilgesellschaftliche und wissenschaftliche Organisationen durch die Bertelsmann Stiftung einbezogen. Darüber hinaus hat das BMI im Jahr 2024 das Projekt „Jahr der Nachricht 2024“gefördert. Das Projekt der UseTheNews gGmbH hat zur Stärkung der Medien- und Nachrichtenkompetenz sowie der gesellschaftlichen Resilienz gegen Desinformation beigetragen.

Zudem ist die Bundeszentrale für politische Bildung (BpB) als fördermittelgebende Institution in diesem Feld aktiv. Die BpB kooperiert seit 2023 mit der „Allianz für Nachrichtenkompetenz im digitalen Zeitalter #UseTheNews“, bei der das Hauptaugenmerk auf der Stärkung junger Menschen im Umgang mit Medien und speziell Nachrichten liegt. Teil der Initiative sind „Newscamps“, die erstmals 2024 mit großem Erfolg durchgeführt wurden und 2025 fortgesetzt werden. Die „Newscamps“ bringen Vertreterinnen und Vertreter der Medienlandschaft, zivilgesellschaftliche Initiativen und junge Zielgruppen zusammen, um an einem gemeinsamen Verständnis eines zeitgemäßen Journalismus zu arbeiten und Resilienzen gegenüber Desinformation und verwandten Phänomenen auszubilden.

In Zusammenarbeit mit den Landesmedienanstalten Berlin-Brandenburg und Nordrhein-Westfalen bietet die BpB den „Newstest“ an. Dieser ermöglicht es Nutzerinnen und Nutzern, selbst zu überprüfen, wie informations- und nachrichtenkompetent sie sind und sich zielgerichtet weiterzubilden. Der „Newstest“ stärkt so die Medienkompetenz der Nutzenden und verringert ihre Anfälligkeit für Manipulationen der demokratischen Öffentlichkeit.

Nach dem Beginn des russischen Angriffskrieges gegen die gesamte Ukraine hat die BpB ihre politischen Bildungsmaßnahmen über russische und pro-russische Desinformation intensiviert. Sie bietet und fördert regelmäßig Projekte mit

wissenschaftlich fundierten Informationen zum Angriffskrieg Russlands gegen die Ukraine, die Desinformationsnarrative dekonstruieren. Dabei bindet sie zivilgesellschaftliche und wissenschaftliche Organisationen ein. Sie veranstaltet jährlich in Kooperation mit nationalen und internationalen Partnerorganisationen Fachkonferenzen zu nationalen und transnationalen Formen von Desinformation und hybrider Kriegsführung für MultiplikatorInnen in der politischen Bildungsarbeit, JournalistInnen und WissenschaftlerInnen. In Kooperation mit dem Zentrum für Osteuropa- und internationale Studien (ZOiS) wurde ein Onlinevideo-Glossar erstellt, das ausgewogene Fachinformationen bietet, die über Ukraine-bezogene Desinformationserzählungen aufklären. Im Rahmen einer Kooperation mit der Stiftung Deutsch-Russischer Jugendaustausch werden Unterrichtsmaterialien für den Schulunterricht entwickelt. Die Themenhefte bieten Informationen und Material, um das Reflexionsvermögen von Lernenden auch gegenüber Desinformationsaktivitäten und -erzählungen zu stärken.

Über das Bundesprogramm „Demokratie leben!“ wurde bis einschließlich 2024 das Projekt „Bundesarbeitsgemeinschaft gegen Hass im Netz“ gefördert. Ziel des Projekts war es, Debattenströme im Netz nachzuzeichnen, Zivilgesellschaft und Wissenschaft im Themenfeld enger zusammenführen und die Arbeit der Zivilgesellschaft im Themenfeld auf eine evidenzbasierte Basis zu stellen. Erfolgreiche Ansätze dieses Projektes werden ab 2025 im Kooperationsverbund gegen Hass im Netz und Desinformation (Arbeitstitel) im Rahmen des Bundesprogramms „Demokratie leben!“ fortgeführt.

BMBF fördert aktuell 15 Forschungsprojekte, die die Erkennung und Bekämpfung von Desinformation zum Gegenstand haben. Die Forschung erfolgt zumeist im Verbund mehrerer Akteure. BMBF hat im Juli 2024 die Förderrichtlinie „Vertrauen in Demokratie und Staat: Digitale Desinformation erkennen und abwehren“ veröffentlicht. Ziel der Förderung ist es, die Forschung, Entwicklung und Innovationskraft im Bereich des Erkennens und Abwehrens von Desinformation nachhaltig zu stärken sowie effektive Lösungen für den Umgang mit Desinformationskampagnen und digitaler Manipulation voranzubringen.

Im Rahmen des aktuellen Programms der Bundesregierung „Forschung für die zivile Sicherheit“ des BMBF wird das Thema „Hybride Bedrohungen“ als eigenes Handlungsfeld adressiert.

Im Rahmen des globalen Einsatzes für Demokratie und Stärkung gesellschaftlicher Resilienz fördert das Auswärtige Amt weltweit zivilgesellschaftliche Projekte. Ziel ist es, die Zivilgesellschaft in den betreffenden Ländern für das Thema Desinformation zu sensibilisieren, die Widerstandsfähigkeit gegen Desinformation zu erhöhen und freien, faktenbasierten Journalismus zu stärken.

Im Rahmen des Förderprogramms zum Schutz und zur strukturellen Stärkung journalistischer Arbeit fördert die Beauftragte der Bundesregierung für Kultur und Medien (BKM) seit 2021 Modellprojekte, die die strukturellen Bedingungen journalistischer Arbeit stärken und zum Schutz des eigenständigen und unabhängigen Journalismus beitragen. Hierüber wird mittelbar in einzelnen Projekten zivilgesellschaftlicher Akteure die Erkennung und Bekämpfung von Desinformationen gefördert. Die BKM fördert zudem Medienkompetenzprojekte, wie beispielsweise im Zeitraum von Januar 2024 bis Dezember 2026 das Projekt „fragFINN erklärt Kindern KI“ des Projektträgers fragFINN e. V.

Von April 2020 bis September 2025 wird aus den Verstärkungsmitteln zur Umsetzung der KI-Strategie der Bundesregierung das Projekt „Künstliche Intelligenz gegen Desinformation (KID)“ der Deutschen Welle gefördert. Dazu gehört die Entwicklung dezidierter KI-Module der „Digitalen Forensik“ zur Verbesserung der (teil)automatisierten Identifizierung von Manipulationen („Fake

News“) an Text, Audio, Fotos und Videos in den (Sozialen) Medien und der Erkennung konzertierter Desinformationskampagnen.

Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 1 und 12 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13542 verwiesen.

27. Wann nimmt die Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM) ihre Arbeit voraussichtlich auf, hat die ZEAM bereits konkrete Fälle von Desinformation bearbeitet, welche Kapazität für die Bearbeitung von Desinformation wird die ZEAM wann voraussichtlich haben, und wie viele Fälle von Desinformation kann diese Stelle voraussichtlich bearbeiten?

29. Mit welchen Institutionen des Bundes und der Länder soll die ZEAM in Austausch treten, und wie wird der Prozess zur Analyse und Information bezüglich Desinformation bei der ZEAM aussehen?

Die Fragen 27 und 29 werden gemeinsam beantwortet.

Zum 1. Juni 2024 hat im BMI eine Projektgruppe zum Aufbau einer „Zentralen Stelle zur Erkennung ausländischer Informationsmanipulation“ (ZEAM) ihre Arbeit aufgenommen. Die ZEAM soll künftig die zentrale Stelle zur Erkennung ausländischer Informationsmanipulation sein. Ziel ist es, die freiheitliche demokratische Grundordnung und damit insbesondere politische Entscheidungsprozesse wie Wahlen vor manipulativer und versteckter Einflussnahme durch fremde Staaten zu schützen.

28. Welche Mechanismen nutzt die Bundesregierung, um die Wirksamkeit ihrer Maßnahmen gegen hybride Angriffe und Desinformation zu evaluieren und auf Basis dieser Erkenntnisse Strategien anzupassen?

Die Bundesregierung beobachtet die Lage kontinuierlich und steht mit allen relevanten Akteuren in einem engen Austausch, um eventuell notwendige Anpassungen von Maßnahmen gegen hybride Angriffe und Desinformation frühzeitig zu erkennen und sicherzustellen. Hierzu gehört auch die Förderung von Forschung und der Austausch mit internationalen Partnern, der Wissenschaft und der Zivilgesellschaft. Das Auswärtige Amt tauscht sich in multilateralen Foren, im Rahmen von EU und NATO sowie in bilateralen Konsultationen mit Partnerstaaten aus.

30. Wie bewertet die Bundesregierung die deutsche Resilienz gegen ausländische Einflussnahme, welche Bedeutung kommt hierbei der Prävention in beispielsweise türkisch- oder russischstämmigen Communitys in Deutschland zu, und welche Maßnahmen unternimmt die Bundesregierung, um migrantische Communitys vor illegitimer Einflussnahme aus dem Ausland, insbesondere aus den Herkunftsstaaten, zu schützen?

Die Bundesregierung arbeitet daran, die Resilienz gegen ausländische Einflussnahme ständig zu verbessern. Dabei sind Formate, die gemeinsam mit benannten Bevölkerungsgruppen entwickelt werden, aus Sicht der Bundesregierung von besonderer Bedeutung. Diese können bedarfs- und phänomengerecht für die jeweils spezifische Zielgruppe entwickelt werden. Die Zusammenarbeit ist zudem wichtige Grundlage, um ausländische Desinformationskampagnen frühzeitig zu erkennen und damit die Resilienz der Gesellschaft in Deutschland insgesamt deutlich zu stärken.

Darüber hinaus kommt Angeboten der politischen Medienbildung eine besondere Bedeutung zu, um Kompetenzen zum kritischen und mündigen Umgang insbesondere mit digitalen Angeboten und Plattformen zu fördern.

Ergänzend wird auf die Antwort zu Frage 31 verwiesen.

31. Welche Bedeutung haben hierbei aus Sicht der Bundesregierung religiöse Einrichtungen und Organisationen, und welche Maßnahmen unternimmt die Bundesregierung, um den ausländischen Einfluss auf religiöse Organisationen zu begrenzen?

Auf der Grundlage des freiheitlichen Religionsverfassungsrechts unterhalten Religionsgemeinschaften in Deutschland vielfältige Beziehungen ins Ausland. Umgekehrt üben religiöse Autoritäten, die ihren Sitz im Ausland haben, Einfluss auf ihnen zugehörige Religionsgemeinschaften in Deutschland aus.

Transnationale Beziehungen sind insbesondere für Religionsgemeinschaften, die sich als Teil von weltweit verbreiteten Religionen verstehen, üblich und verfassungsrechtlich geschützt.

Die Bundesregierung verfolgt integrationspolitisch das Ziel, dass Religionsgemeinschaften, deren religiöse Autoritäten ihren Sitz im Ausland haben, sich eigenständig und unabhängig von möglicher illegitimer Einflussnahme aus dem Ausland organisieren. So ist es ein Ziel der Deutschen Islam Konferenz (DIK), dass islamische religiöse Gemeinschaften in Deutschland ihr religiöses Personal selbst und auf Deutsch ausbilden. Aus Mitteln der DIK werden hierzu Projekte der Ausbildung religiösen Personals islamischer Gemeinden gefördert. Um die Ausbildung in Deutschland auch strukturell zu befördern, hat die DIK im November 2025 eine Handreichung der Anerkennung der Berufe und Ausbildungsgänge religiösen Personals islamischer Gemeinden publiziert (vgl. www.deutsche-islam-konferenz.de/SharedDocs/Meldungen/DE/ImDialog/241118-dik-handreichung-2024.html).

Ergänzend haben sich das BMI, die türkische Religionsbehörde Diyanet und die Türkisch-islamische Union der Anstalt für Religion e. V. (DITIB) im Dezember 2023 auf eine schrittweise Beendigung der Entsendung staatlich bediensteter islamischer Religionsbeauftragter aus der Türkei nach Deutschland geeinigt. Im Rahmen einer gemeinsamen Ausbildungsinitiative sollen pro Jahr 100 islamische Religionsbeauftragte, die als Vorbeter und Prediger in Gemeinden der Türkisch-Islamischen Union der Anstalt für Religion e. V. (DITIB) tätig werden sollen, in Deutschland ausgebildet und die Entsendung aus der Türkei schrittweise in gleicher Stärke reduziert werden (vgl. www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/12/imam-ausbildung.html#:~:text=Das%20Bundesinnenministerium%2C%20die%20t%C3%BCrkische%20Religionsbeh%C3%B6rde,der%20T%C3%BCrkei%20nach%20Deutschland%20geeinigt). Auf dieser Grundlage wird derzeit und gefördert aus Mitteln der DIK ein neuer Ausbildungsgang konzipiert.

32. Welche Strategien anderer EU-Mitgliedstaaten zur Bekämpfung von hybriden Angriffen und Desinformation hat die Bundesregierung im Rahmen einer Best-Practice-Auswertung ausgewertet, und um welche Mitgliedstaaten handelt es sich insoweit?

Die Bundesregierung beobachtet die Ansätze von Partnerstaaten zum Umgang mit hybriden Bedrohungen und steht mit diesen im Austausch.

Die Bundesregierung steht zum Schutz vor Desinformation in engem Austausch mit EU-Partnern. Von besonderer Bedeutung ist hierbei die Horizontal

Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT). Zudem besteht eine enge Kooperation im Rahmen des EU-Rapid-Alert-Systems sowie im Weimar alert scheme mit Polen und Frankreich. Das Auswärtige Amt hat wiederholt Konsultationen mit europäischen Partnern geführt, bei denen der Austausch über Strategien zur Bekämpfung von Desinformation und anderen hybriden Bedrohungen ein wichtiges Element war. Zuletzt fanden solche Konsultationen z. B. mit den drei baltischen Staaten im Dezember 2024 in Riga statt.

33. Welche Maßnahmen dieser Staaten zur Bekämpfung von hybriden Angriffen und Desinformation sind aus Sicht der Bundesregierung auf Deutschland übertragbar und würden einen Mehrwert bei der Abwehr solcher Angriffe ergeben, und wie bewertet die Bundesregierung insbesondere

    a) die französische Beobachtungsstelle für digitale Einflussnahme aus dem Ausland „Viginum“,

    b) die schwedische Behörde für psychologische Verteidigung,

    c) die schwedische Initiative, die Zivilbevölkerung auch durch Flugblätter über Zivil- und Katastrophenschutz aufzuklären,

    d) das finnische Programm zur Schaffung und zum Erhalt von Schutzräumen für große Teile der Zivilbevölkerung,

    e) die Strategie der Königlich Dänischen Marine zur Festsetzung von Schiffen, die im Verdacht stehen, Unterseekabel in der Ostsee beschädigt zu haben,

    f) das niederländische Programm „Mediawijsheid“ (Medienkompetenz), durch welches die Medienkompetenz in Schulen und Kindergärten gefördert wird,

    g) die in Polen eingerichtete Task Force zur strategischen Kommunikation „Departament Komunikacji Strategicznej i Przeciwdziałania Dezinformacji Międzynarodowej“ zur Bekämpfung internationaler Desinformation?

Die Bundesregierung begrüßt Bemühungen ihrer EU-Partner und NATO-Alliierten, hybriden Bedrohungen einschließlich Desinformation wirksam zu begegnen. Eine Bewertung der Maßnahmen anderer Mitgliedstaaten durch die Bundesregierung erfolgt nicht.

34. Wie bewertet die Bundesregierung die Strategie der britischen Nachrichtendienste und des britischen Verteidigungsministeriums, durch sogenannte strategic declassification Fake News und Desinformation entgegenzuwirken und insbesondere mit Blick auf die Ukraine faktenbasierte Informationen zu veröffentlichen, plant die Bundesregierung vergleichbare Informationskampagnen?

Die Bundesregierung steht in engem und laufendem Austausch mit EU-Partnern und NATO-Alliierten zur Entwicklung eigener und gemeinsamer Maßnahmen. Die Bundesregierung bewertet keine Maßnahmen anderer Staaten. Die öffentliche Kommunikation und das Teilen faktenbasierter Informationen ist grundsätzlich Handlungsgrundlage für die politische Kommunikation. Dabei kann auch „strategic declassification“ Anwendung finden.

35. Welche Erkenntnisse hinsichtlich ausländischer Einflussnahme hat die Bundesregierung aus den letzten beiden US-Präsidentschaftswahlen und der letzten Wahl zum Deutschen Bundestag gezogen, welche Angriffsmuster hat die Bundesregierung hierbei identifiziert, und welche Akteure stecken hinter den festgestellten Angriffen?

Im Vorfeld der Bundestagswahl 2021 gab es Versuche Russlands, indirekt Einfluss auf die Wahl auszuüben. Russland verbreitete insbesondere Desinformation und Propaganda. Darüber hinaus wird auf die Antwort der Bundesregierung zu Frage 14 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/12872 verwiesen.

Die Bundesregierung steht in engem Austausch mit der US-Regierung zu ausländischer Einflussnahme im Rahmen von Wahlen. Darüber hinaus wird auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der AfD-Fraktion auf Bundestagsdrucksache 20/14469 verwiesen.

36. Mit welcher Art von Beeinflussung und ausländischer Einflussnahme auf die kommende Wahl zum Deutschen Bundestag rechnet die Bundesregierung, welches Konzept zur Verhinderung dieser Einflussnahme verfolgt die Bundesregierung, und welche Maßnahmen hat sie insoweit bereits getroffen bzw. wird diese bis zum Wahltermin noch treffen?

Zentrale politische Ereignisse wie die Durchführung von Wahlen können stets Zielscheibe von unzulässiger Einflussnahme fremder Staaten werden, die so ihre strategischen Ziele verfolgen wollen. Die Bundesregierung geht davon aus, dass entsprechende Einflussmaßnahmen im Kontext der Bundestagswahl 2025 für manche Staaten als Handlungsoptionen infrage kommen. Einzukalkulieren sind Aktionen der Desinformation und Diskreditierung, Cyberangriffe sowie Spionage und Sabotage.

Im Übrigen wird auf die Antwort zu Frage 7 verwiesen.

37. Welche Maßnahmen hat die Bundesregierung getroffen, um der Gefahr durch sogenannte Deepfakes und andere KI-generierte Inhalte im Vorfeld der kommenden Wahl zum Deutschen Bundestag zu begegnen?

Es wird auf die Antwort zu Frage 7 verwiesen.

Prebunking und KI-bezogene Medienkompetenztrainings stellen aus Sicht der Bundesregierung sinnvolle Maßnahmen im Sinne der Prävention, des Aufbaus von gesamtstaatlicher und gesellschaftlicher Resilienz sowie der Sensibilisierung der Öffentlichkeit zur Erkennung von sowie im Umgang mit KI-Inhalten dar. In diesem Sinne hat die BpB im Rahmen des „Aktionsplan gegen Rechtsextremismus“ explizit Projekte in die Förderung aufgenommen, die Desinformation auf Plattformen in sozialen Netzwerken mit Prebunking und Digital-Streetwork-Konzepten begegnen.

Zudem hat die BpB Anfang Dezember 2024 das an Multiplikatorinnen und Multiplikatoren gerichtete Online-Dossier „Wenn der Schein trügt – Deepfakes und die politische Realität“ zum Thema KI und Deepfakes veröffentlicht. Das Online-Dossier macht auf die hinter Deepfakes stehenden Mechanismen und Funktionsweisen aufmerksam, informiert über Einsatzfelder von KI und Deepfakes und sensibilisiert für Potenziale und Gefahren für die Demokratie. Das Angebot qualifiziert Lehrkräfte und Fachkräfte der Sozialen Arbeit und politischen Bildung für die Arbeit mit Jugendlichen und jungen Erwachsenen zu dem Themen- und Handlungsfeld. Ende Januar 2025 veröffentlicht die BpB Unterrichtmaterialien zu Deepfakes und Wahlen, die Lehrkräften eine vertiefte

Auseinandersetzung im Schulunterricht mit den Gefahren von Deepfakes im Kontext von Wahlen ermöglichen.

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.bundesanzeiger-verlag.de
ISSN 0722-8333