Deutscher Bundestag **Drucksache 21/995**

21. Wahlperiode 24.07.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Agnieszka Brugger, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 21/769 –

Fragen zur Notwendigkeit eines umfassenden Lagebilds zu Sabotage, Spionage und Desinformation

Vorbemerkung der Fragesteller

Die Bundesrepublik Deutschland, ihre demokratischen Institutionen, aber auch ihre Lebensadern, die kritischen Infrastrukturen (KRITIS), sind seit Jahren sehr ernsten Angriffen, auch und vor allem ausländischer Nachrichtendienste und ihr nahestehender Gruppierungen ausgesetzt. Der russische Angriffskrieg gegen die Ukraine wirkte dabei als Katalysator für die feindlichen nachrichtendienstlichen Tätigkeiten des russischen Regimes unter Wladimir Putin. Es ist ein deutlicher Anstieg sicherheitsrelevanter russischer Aktivitäten in Europa und besonders auch in Deutschland zu verzeichnen. Spionage, Sabotage und Desinformationskampagnen bilden dabei zentrale Elemente zahlreicher fast täglich stattfindender hybrider Angriffe, die sich gezielt gegen politische Institutionen, kritische Infrastrukturen und den öffentlichen Diskurs richten und dadurch zunehmend die gesellschaftliche Stabilität gefährden. Auf diese eklatant gestiegenen Angriffe und die Notwendigkeit, rechtsstaatlich entschlossen auf sie zu reagieren, machen auch Vertreter deutscher Sicherheitsbehörden und der Nachrichtendienste seit Langem vehement aufmerksam. Das Bundesamt für Verfassungsschutz (BfV) stellt in seinem kürzlich veröffentlichten Jahresbericht eine zunehmende Offenheit, Aggressivität und strategische Vielfalt russischer Operationen gegen die Grundpfeiler unserer freiheitlich-demokratischen Gesellschaft fest (www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html).

Diese Entwicklungen sind jedoch nicht isoliert zu betrachten, sondern stehen im Kontext einer umfassenderen Bedrohung durch das zunehmend aggressive Verhalten von Putins Russland und insbesondere seiner verdeckt operierenden Geheimdienste und ihnen nahestehender Gruppierungen. Deren Agieren wird immer aggressiver. Sie schrecken selbst vor schweren Straftaten nicht zurück. Davon zeugen verschiedene Verfahren, die der Generalbundesanwalt (GBA) derzeit führt. Auch bei der letzten öffentlichen Anhörung der Nachrichtendienste durch das Parlamentarische Kontrollgremium (PKGr) am 14. Oktober 2024 warnten deren Spitzen ausdrücklich vor Russlands imperialistischer Expansionspolitik (www.bundestag.de/dokumente/textarchiv/2024/kw42-pa-pkg

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 24. Juli 2025 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

r-1020558). Insbesondere der Bundesnachrichtendienst und sein (noch) amtierender Präsident Bruno Kahl warnten zuletzt öffentlich davor, dass Russland sogar die Reaktionsmechanismen des NATO-Bündnisses – namentlich den Artikel 5 des NATO-Vertrages – auf die Probe stellen wird (www.tagesspiegel.de/internationales/haben-nachrichtendienstliche-belege-bnd-chef-kahl-warnt-vor-russischem-angriff-auf-nato-staaten-13834069.html).

Dabei ist ein Schlüsselelement im Baukasten der hybriden russischen Angriffe gegen den Westen – aber auch sonstiger, insbesondere chinesischer Akteure – die Spionage. Ziel dieser Aktivitäten ist es, Informationen aus sensiblen Bereichen wie Politik, Militär, Wirtschaft, Forschung und kritischer Infrastruktur zu gewinnen. Neben der klassischen Spionage – durch Nutzung menschlicher Quellen – kommt dabei auch Cyberangriffen eine herausragende Bedeutung zu. Letztere verursachen nach Erhebungen des Branchenverbandes BITKOM – die nach Auffassung des BfV-Vizepräsidenten Sinan Selen noch immer nicht einmal die Realität widerspiegeln – wirtschaftliche Schäden in dreistelliger Milliardenhöhe (www.rnd.de/wirtschaft/bitkom-wirtschaftsschutzbericht-ueber-cyberangriffe-und-spionage-schaeden-bei-unternehmen-auf-WLMC7BDRXRBLTDP54CQJSJVTW4.html), haben aber auch immer wieder das Ziel, sicherheitsrelevante Information zu extrahieren, und gefährden damit aktiv und mit wachsender Bedrohlichkeit auch die nationale Sicherheit. Auch durch journalistische („Vulcan-Files“) Recherchen wissen die Fragesteller, dass alle EU-Mitgliedstaaten im Fokus der Angreifer stehen, Deutschland als Land im Herzen Europas und einer der wichtigsten Unterstützer der Ukraine jedoch ganz besonders. Ebenso besorgniserregend sind regelmäßig auftretende Drohnenüberflüge über Kasernen, militärische Einrichtungen, Marineanlagen sowie über Anlagen der kritischen Infrastruktur (www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html oder zur KRITIS www.ndr.de/fernsehen/sendungen/panorama3/meldungen/Drohnen-ueber-Norddeutschland-Kritische-Infrastruktur-im-Visier,drohnen442.html). Bislang nicht ausreichend erfasst scheint nach Ansicht der Fragesteller zudem das Ausmaß rechtswidriger Zutritte und Einbrüche in KRITIS-Anlagen und sensible Rüstungsunternehmen. Betreiber berichten, auch gegenüber den Fragestellern, von einem besorgniserregenden und nicht allein durch Private abwehrbaren Ausmaß, in dem sie aufgebrochene Türen und Fenster, Löcher in Zäunen, maskierte Personen im Umfeld der Anlagen und Ähnliches registrieren. Diese Vorfälle deuten darauf hin, dass systematisch nach Schwachstellen in der deutschen Verteidigungs- und Sicherheitsarchitektur gesucht wird, um diese zu identifizieren und für eigene Zwecke nutzbar zu machen.

Zudem ist eine ähnliche Entwicklung auch im Hinblick auf Sabotageaktivitäten zu beobachten. Diese zeichnet sich sowohl im Hinblick auf die Vielfalt der eingesetzten geheimdienstlichen Methoden als auch der Bandbreite potenzieller Zielobjekte aus. So sind gezielte Tötungen im öffentlichen Raum – wie etwa der Tiergarten-Mord – sowie strategisch vorbereitete Anschlagspläne gegen Führungspersonal der deutschen Rüstungsindustrie dokumentiert. Besonders alarmierend ist der verstärkte Einsatz niedrigschwellig rekrutierter Handlanger – sogenannter Low-Level-Agenten (oder auch Wegwerfagenten) –, die gezielt zur Ausführung von Störaktionen für kleines Geld angeheuert und eingesetzt werden. Darüber hinaus sind auch Sabotageakte, etwa mittels Brandsätze, gegen Energie-, Verkehrs- und Militäreinrichtungen mit mutmaßlich nachweislich russischer Handschrift zu verzeichnen (www.tagesspiegel.de/politik/dhl-paketbrand-in-leipzig-sabotage-akt-vom-juli-hatte-offenbar-fast-zu-flugzeugabsturz-gefuhrt-12528386.html; www.morgenpost.de/vermischtes/article242247132/Grossbrand-in-Berlin-Firma-stellt-Waffen-fuer-Ukraine-her.html).

Eng verknüpft mit diesen physischen Angriffen auf gesellschaftliche Stabilität ist eine weitere digitale Dimension hybrider Kriegsführung: die gezielte Verbreitung von Desinformation. Während Sabotageakte unmittelbar sichtbare Schäden anrichten, entfalten Desinformationskampagnen ihre Wirkung oft schleichend – und sind dabei nicht minder gefährlich für den gesellschaftlichen Zusammenhalt und die demokratische Ordnung. Russland und seine Proxies verbreiten dazu bewusst und zielgerichtet falsche oder irreführende Infor-

mationen bzw. verschweigen und verschleiern wesentliche Teile einer Information. Sie nutzen für die Verbreitung von Desinformation den gesamten Informationsraum, also alle digitalen und analogen Kanäle, Medien und Formate. Damit will man gezielt und vorsätzlich Menschen und die Öffentlichkeit täuschen, beeinflussen und verunsichern, die öffentliche Meinungsbildung manipulieren, kontroverse Debatten zusätzlich emotionalisieren, gesellschaftliche Spannungen verstärken und Misstrauen in staatliche Institutionen und Regierungshandeln schüren. Die Kampagnen greifen dabei häufig emotional aufgeladene oder polarisierende Themen auf und verbreiten gezielt Falschinformationen – etwa über prominente politische Akteure, wie im Fall der Falschbehauptung über einen angeblichen Kokainkonsum von Emmanuel Macron (www.spiegel.de/ausland/emmanuel-macron-versteckt-taschentuch-russland-spinnt-daraus-koks-vorwurf-a-0162d96e-c9f4-47ce-871b-a73e235d2032). Besonders besorgniserregend ist, dass solche Narrative nicht nur über russische Kanäle verbreitet werden, sondern zunehmend auch von inländischen Akteuren oder sogenannten Trollbots aufgegriffen und weiterverbreitet werden, wodurch eine gefährliche Wechselwirkung zwischen ausländischer Einflussnahme und innergesellschaftlicher Radikalisierung entsteht, die den öffentlichen Diskurs massiv beeinflusst und das demokratische Gemeinwesen nachhaltig destabilisiert.

Zugleich sticht neben den russischen feindlichen Attacken gegen die Bundesrepublik Deutschland wie in anderen westlichen und demokratischen Gesellschaften die Volksrepublik China aufgrund ihrer Operationen im Bereich der Spionage und Einflussnahme in Deutschland hervor. Diese stellen sowohl quantitativ und qualitativ sowohl mit ihrem, wie es das Bundesamt für Verfassungsschutz (BfV) betont, „All-Tools-and-All-Sectors-Approach“ (www.verfassungsschutz.de/SharedDocs/hintergruende/DE/wirtschafts-wissenschaftsschutz/chinas-neue-wege-der-spionage.html) als auch mit Blick auf die langfristige Strategie, die Quantität und Qualität der Attacken ebenfalls eine besondere Gefahr dar, die auch nach Ansicht der Fragesteller deutlich mehr an Aufmerksamkeit und ein erhöhtes Maß an Schutzmaßnahmen, unter anderem auch im Wissenschaftsbereich, dringend erforderlich macht.

All diese Entwicklungen verdeutlichen das Ausmaß, in dem Deutschland im Zentrum hybrider Angriffe, insbesondere aus Russland, aber auch aus mehreren anderen autoritären Staaten, steht. Eine echte Zeitenwende auch in der inneren Sicherheit und die schnellstmögliche Erhöhung gesellschaftlicher Resilienz gegenüber der stark gestiegenen Bedrohung bleiben das Gebot der Stunde. Die Erweiterung des Sicherheitsbegriffs im Rahmen der Änderungen der Finanzverfassung waren auch nach Meinung der Fragesteller ein entscheidender Schritt. Weitere müssen dringend folgen. Die neuen finanziellen Möglichkeiten müssen schnell und effektiv genutzt werden. Denn: Es braucht dringend eine moderne, vorausschauende und auf Resilienz ausgerichtete Innen-, Sicherheits- und Verteidigungspolitik. Der Umgang und das Zusammenführen wichtiger Informationen innerhalb der Bundesregierung ist dafür ein herausragend wichtiger Baustein; eine zentrale, ressort- und Bund-Länder-übergreifende Koordinierung und Bündelung sicherheitsrelevanter Erkenntnisse ist nach Einschätzung der Fragesteller bislang jedoch nicht erkennbar. Um hybride Angriffe und Desinformation effektiv erkennen und abwehren zu können, ist dies aber zwingend erforderlich, insbesondere um das Ausmaß der Angriffe überhaupt absehen zu können, um Muster zu erkennen und mögliche politische und gesetzgeberische Handlungsnotwendigkeiten identifizieren zu können. Eine resiliente Gesellschaft ist zudem zwingend auf gut informierte und wachsame Bürgerinnen und Bürger angewiesen. Dies kann nur durch eine gänzlich andere Ansprache durch die Spitzen der Bundesregierung erreicht werden. Auch dafür könnte ein Gesamtlagebild „Nationale Sicherheit“ ein wichtiger Baustein sein.

Vorbemerkung der Bundesregierung

1. Die in der vorliegenden Anfrage aufgeführten Einzelphänomene (u. a. Sabotage, Spionage, Cyberangriffe, Desinformation) werden, sofern sie ausländische staatliche Urheber haben, seitens der Bundesregierung als „hybride Bedrohungen“ geführt und bearbeitet. Hybride Bedrohungen bezeichnen koordinierte, illegitime Handlungen staatlicher und staatlich gelenkter Akteure zur Durchsetzung eigener Interessen zum Nachteil eines anderen Staates, die außerhalb des Rahmens eines konventionellen militärischen Angriffs bleiben. Federführendes Ressort innerhalb der Bundesregierung für den Umgang mit hybriden Bedrohungen ist das Bundesministerium des Innern (BMI). Das BMI ist für die ressort- sowie Bund-Länder-übergreifende Koordinierung und Bündelung von Erkenntnissen verantwortlich.

Um ein gemeinsames Vorgehen der Ressorts auf nationaler Ebene sicherzustellen, wird in der „Arbeitsgruppe Hybride Bedrohungen“ (AG Hybrid) unter Leitung des BMI der strategische Umgang mit hybriden Bedrohungen koordiniert. Auf Arbeitsebene ist die vom BMI geleitete „Task Force gegen Desinformation und weitere hybride Bedrohungen“ tätig. Beide Gremien umfassen alle Ressorts und u. a. die Sicherheitsbehörden. Die Task Force koordiniert auch den Schutz von Wahlen vor hybriden Bedrohungen einschließlich Desinformation.

Für eine Stärkung des Informationsaustauschs zwischen Bundesressorts, Sicherheitsbehörden des Bundes, Ländern und kommunalen Spitzenverbänden sorgt unter Federführung des BMI eine Bund-Länder-offene Arbeitsgruppe Hybride Bedrohungen in der Struktur der Innenministerkonferenz (IMK). Hier werden u. a. die Auswirkungen hybrider Bedrohungen auf die Länder einschließlich ihrer Kommunen erörtert.

Auf internationaler Ebene kooperiert die Bundesregierung beim Umgang mit hybriden Bedrohungen in verschiedenen bi- und multilateralen Formaten. In diesen Formaten findet ein regelmäßiger Informations- und Erfahrungsaustausch statt. Einen Schwerpunkt bildet dabei die Zusammenarbeit auf EU-Ebene, innerhalb der NATO und den G7.

Der parlamentarische Raum wird von der Bundesregierung zu hybriden Bedrohungen informiert. Die Bundesregierung hat z. B. Informationsmaterialien zu hybriden Bedrohungen und Schutzmaßnahmen im Kontext der Bundestagswahl 2025 bereitgestellt.

Auch die Öffentlichkeit wird mittels vielfältiger Informationsmaterialien zu hybriden Bedrohungen sensibilisiert.

Unter Federführung des BMI erstellt die Bundesregierung in der Regel alle zwei Wochen den Lagebericht Hybride Bedrohungen, der als „VS-Nur für den Dienstgebrauch“ (VS-NfD) eingestuft ist. Darin finden sich u. a. Beiträge zu Bedrohungen im Informations- und Cyberraum sowie zu Spionage und Sabotage. Der Lagebericht Hybride Bedrohungen wird den Bundesressorts und nachgeordneten Behörden sowie den Ländern zur Information und Sensibilisierung zur Verfügung gestellt.

Die Frage nach einzelnen und/oder gebündelten „Lagebildern“ zieht sich durch die vorliegende Anfrage. Dieser Begriff ist jedoch nicht einheitlich definiert und wird je nach Akteur und Ebene unterschiedlich verstanden. Grundsätzliches Ziel eines Lagebildes ist nach Auffassung der Bundesregierung, den Verantwortlichen auf den unterschiedlichen, administrativen Ebenen eine valide Informationsbasis und Entscheidungsgrundlage für ihr Handeln zu bieten. Derzeit erarbeiten das Bundesamt für Verfassungsschutz (BfV) und das Bundeskriminalamt (BKA) im Auftrag von AK II und AK IV ein sogenanntes Lagebild „Hybride Bedrohungen“, welches zur Herbstsitzung der IMK 2025 vorzulegen ist und die Phänomenbereiche Desinformation, Proliferation, Spionage, Sabota-

ge und Staatsterrorismus umfassen soll. Dieses Lagebild scheint für die fachlich erforderliche Bewertung und fortlaufende Betrachtung geeignet und führt operative Erkenntnisse zu den genannten Einzelphänomenen zusammen. Es umfasst allerdings bei weitem nicht alle Facetten hybrider Bedrohungen.

2. Die Bundesregierung ist nach sorgfältiger Abwägung zu dem Ergebnis gelangt, dass eine Beantwortung der Fragen 1 und 3 aus Gründen des Staatswohls nicht, auch nicht in eingestufter Form, erfolgen kann. Die öffentliche Beantwortung der Fragen würde Zahlen in solch detaillierter Form darlegen, dass daraus unmittelbar oder mittelbar Rückschlüsse auf etwaige Aufklärungsfähigkeiten sowie die Einsatzbereitschaft der Drohnenabwehr der Bundeswehr gezogen werden können. Eine Preisgabe dieser Informationen könnte schwerwiegende Nachteile bei der Aufklärung und Abwehr von Spionage und Sabotage mit sich bringen und damit zu einer erheblichen Gefährdung militärischer Liegenschaften und des Bundeswehrpersonals führen. Unbefugte Dritte könnten daran ihre eigenen Maßnahmen zum Nachteil der Bundeswehr und somit der Bundesrepublik Deutschland ausrichten. Durch die Kenntnis der Informationen könnten ggf. auch Schwachstellen der Streitkräfte aufgedeckt werden, deren Kenntnis zum Nachteil der Einsatz- und Verteidigungsbereitschaft der Bundeswehr genutzt werden könnten. Daraus können erhebliche negative Folgewirkungen für die Sicherheitslage in der Bundesrepublik Deutschland entstehen.

Auch eine Einstufung und Hinterlegung der angefragten Informationen zu Vorkommnissen in Bezug auf militärische Liegenschaften, Einrichtungen und Anlagen als Verschlusssache beim Deutschen Bundestag würde der Bedeutung der Informationen in Hinblick auf die Verteidigungsbereitschaft und Aufklärungsfähigkeiten der Bundeswehr und somit den Sicherheitsinteressen der Bundesrepublik Deutschland nicht ausreichend Rechnung tragen. Selbst eine Bekanntgabe gegenüber dem begrenzten Kreis von Empfängern kann dem Schutzbedürfnis nicht hinreichend Rechnung tragen, da auch nur die geringe Gefahr des Bekanntwerdens nicht hingenommen werden kann. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart besonders schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

3. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Beantwortung der Fragen 2, 4 und 5e aus Gründen des Staatswohls ausnahmsweise nicht offen erfolgen kann. Eine Offenlegung selbst scheinbar abstrakter Zahlenwerte – wie etwa der Anzahl der Vorkommnisse, in denen bestimmte nachrichtendienstliche oder polizeiliche Mittel eingesetzt wurden – kann Rückschlüsse auf die technischen Fähigkeiten, den Ressourceneinsatz, den strategischen Fokus sowie bestehende Erkenntnislagen der Bundessicherheitsbehörden zulassen. So kann etwa durch die Veröffentlichung von Daten mehrerer aufeinanderfolgender Jahre ein Profil der Ermittlungsintensität und Prioritätensetzung einzelner Kriminalitätsbereiche entstehen. Ferner sind die Informationen bei Kenntnisnahme durch Unbefugte auch dazu geeignet, Rückschlüsse auf Kapazitäten und Fähigkeiten der Bundeswehr zuzulassen. Gerade in Bereichen, in denen eine fremde Macht involviert ist, können solche Informationen die Gegenseite in die Lage versetzen, Handlungen gezielt anzupassen, Beweismittel zu verschleiern oder Ermittlungen zu unterlaufen. Die Antwort zu den genannten Fragen wird daher als Verschlusssache gemäß der VSA mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

4. Ferner ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 5a bis 5d, 13 bis 13c und 16 bis 16d auf Grund des unzumutbaren Aufwandes, der mit einer Antwort ver-

bunden wäre, nicht erfolgen kann. Das Bundesverfassungsgericht (BVerfG) hat in ständiger Rechtsprechung bestätigt, dass das parlamentarische Informationsrecht unter dem Vorbehalt der Zumutbarkeit steht (BVerfG, Urteil vom 7. November 2017 – 2 BvE 2/11 –, BVerfGE 147, 50, 147 f.). Danach sind nur die Informationen mitzuteilen, über die die Bundesregierung verfügt oder die sie mit zumutbarem Aufwand in Erfahrung bringen kann. Die Kriterien im Sinne der Fragestellungen sind keine, die in den Verfahrensregistern des Generalbundesanwalts beim Bundesgerichtshof (GBA) geführt werden. Erforderlich wäre daher eine händische Auswertung eines immensen Aktenbestandes. Selbst bei digitalisierten Aktenbeständen müsste eine manuelle Suche zusätzlich erfolgen, da auch mittels Abfrage einzelner Suchbegriffe keine vollständige Trefferliste garantiert werden könnte. Die zur Beantwortung der Fragen notwendige Recherche würde die entsprechenden Arbeitseinheiten beim GBA für einen erheblichen Zeitraum in einer Weise beanspruchen, dass diesen eine ordnungsgemäße Erledigung ihrer Ermittlungsaufgaben nicht mehr möglich wäre. Auch weist die Bundesregierung darauf hin, dass etwa verdeckt geführte Ermittlungsverfahren nicht – auch nicht in eingestufter Form – beauskunftet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird insoweit durch das aus dem Rechtsstaatprinzip abgeleitete und damit gleichfalls Verfassungsrang genießende schutzwürdige Interesse der Allgemeinheit an der Gewährleistung einer funktionsgerechten und organadäquaten Aufgabenwahrnehmung durch die Strafverfolgungsbehörden begrenzt. Eine Auskunft würde konkret weitergehende Ermittlungsmaßnahmen erschweren oder gar vereiteln. Nach sorgfältiger und konkreter Abwägung der betroffenen Belange tritt das Informationsinteresse des Parlaments daher hinter die ebenso berechtigten Interessen an einer effektiven Strafverfolgung zurück. Im Übrigen weist die Bundesregierung darauf hin, dass zu auf Landesebene geführten Verfahren aufgrund der vom Grundgesetz vorgegebenen Kompetenzordnung grundsätzlich keine Stellung genommen wird.

5. Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die Beantwortung der Frage 9 wegen des unzumutbaren Aufwandes, der mit der Beantwortung verbunden wäre, nicht erfolgen kann. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung bestätigt, dass das parlamentarische Informationsrecht unter dem Vorbehalt der Zumutbarkeit steht (BVerfG, Urteil vom 7. November 2017 – 2 BvE 2/11 –, BVerfGE 147, 50, 147 f.). Es sind alle Informationen mitzuteilen, über die die Bundesregierung verfügt oder die sie mit zumutbarem Aufwand in Erfahrung bringen kann. Eine Quantifizierung relevanter Sachverhalte ist nicht möglich. Ab wann eine Betroffenheit als Cyberangriff gewertet werden kann, ist hier unklar und weder in der Fragestellung noch grundsätzlich definiert. Die mögliche Spannweite einer Begriffsbeschreibung reicht von einem Zugang einer Phishing-Mail bei einem Betroffenen bis hin zu einem nachweislich eingetretenen tatsächlichen und erheblichen Schadensereignisses (im Bereich der Informationssicherheit gleichbedeutend mit dem Verlust von mindestens der Integrität oder der Vertraulichkeit oder der Verfügbarkeit von Daten/IT-Infrastruktur). Auch dies berücksichtigend wird keine laufende statistische Erfassung vorgenommen. Selbst bei hinreichender Begriffsbestimmung müsste jeder Sachverhalt händisch nach Aktenlage geprüft werden. Der mit der händischen Suche verbundene Aufwand würde die Ressourcen allein im Bereich der Spionageabwehr für einen nicht absehbaren Zeitraum vollständig beanspruchen und ihre Arbeit zum Erliegen bringen. Die Aussagekraft der ermittelten Zahlen wäre noch dazu gering, da hier von einer enormen Dunkelziffer ausgegangen werden muss. Die Cyberabwehr des BfV bearbeitet fokussiert Einzelsachverhalte, es muss allerdings von einem Massenphänomen ausgegangen werden. Das darauf basierende Lagebild kann zwar so qualifizierte Aussagen über den Modus Operandi staatlich gesteuerter

Cyberakteure liefern, mögliche betroffene Branchen identifizieren, Trends erkennen und die Herkunft und Interessenlage der Angreifer analysieren. Eine umfassende Aussage zur exakten Anzahl kann jedoch so nicht erfolgen.

1. Wie viele Fälle des unerlaubten Betretens, Ausspähens oder physischen Manipulierens, Beschädigens und Einbrechens von und in Kasernen, militärische Einrichtungen und Marineanlagen auf deutschem Bundesgebiet sind der Bundesregierung seit dem Jahr 2022 bekannt geworden (bitte nach Jahren aufschlüsseln)?

Die Bundesregierung verweist auf ihren 2. Punkt der Vorbemerkung.

2. Wie viele Fälle des unerlaubten Betretens, Ausspähens oder physischen Manipulierens, Beschädigens und Einbrechens von und in KRITIS-Anlagen sind der Bundesregierung seit dem Jahr 2022 bekannt geworden (bitte nach Jahren aufschlüsseln)?

Die Bundesregierung verweist auf ihren 3. Punkt der Vorbemerkung.

3. Wie viele Fälle von Drohnen(über-)flügen über Kasernen, militärischen Einrichtungen und Marineanlagen auf deutschem Bundesgebiet sind der Bundesregierung seit dem Jahr 2022 bekannt und dokumentiert worden (bitte nach Einrichtungen und Jahren aufschlüsseln)?

Die Bundesregierung verweist auf ihren 2. Punkt der Vorbemerkung.

4. Wie viele Fälle von Drohnen(über-)flügen über KRITIS-Einrichtung und Anlagen sind der Bundesregierung seit dem Jahr 2022 bekannt und dokumentiert worden (bitte nach Einrichtungen und Jahren aufschlüsseln)?

Die Bundesregierung verweist auf ihren 3. Punkt der Vorbemerkung.

5. Bitte jeweils differenziert mit Bezug auf die Fragen 1 bis 4:
   a) In wie vielen Fällen wurden strafrechtliche Ermittlungen eingeleitet?
   b) In wie vielen Fällen konnten tatverdächtige Personen ermittelt werden?
   c) In wie vielen Fällen kam es zur Anklage?
   d) In wie vielen Fällen konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)?

Die Fragen 5a bis 5d werden gemeinsam beantwortet.

Die Bundesregierung verweist auf ihren 4. Punkt der Vorbemerkung.

   e) Bestehen aus Sicht der Bundesregierung rechtliche oder faktische Defizite, die die Aufklärung von in den Fragen 1 bis 4 erfragten Fällen besonders erschweren, und wenn ja, welche?

Die Bundesregierung verweist auf ihren 3. Punkt der Vorbemerkung.

6. Bei welchen landes- und bundesbehördlichen Stellen liegen nach Kenntnis der Bundesregierung Informationen über die in den Fragen 1 bis 4 erfragten Fälle vor, und bei welchen Stellen oder Zentren laufen diese zusammen?

Das Lagezentrum des BMI beobachtet rund um die Uhr sicherheitsrelevante Ereignisse in Deutschland und dem Ausland, sofern die Sicherheitslage im Inland oder deutsche Interessen betroffen sein könnten. In enger Abstimmung mit dem Bundeskanzleramt, den Bundesressorts und den Landesinnenministerien werden relevante Informationen ausgetauscht, analysiert und erstbewertet. Daraus entstehen unterschiedliche Lageprodukte und ad-hoc Briefings, zum einen für das BMI, zum anderen für die Länder. Dazu zählt auch der „VS-Nur für den Dienstgebrauch“ (VS-NfD) eingestufte Lagebericht Innere Sicherheit (gemäß Umlaufbeschluss des UA FEK vom 4. Juli 2012 und Umlaufbeschluss des AK II der IMK vom 27. Juli 2012), der täglich erscheint und die Sicherheitslage im Berichtszeitraum der vergangenen 24 Stunden abdeckt. Dieser beinhaltet neben der polizeilichen Lage u. a. auch den Unterpunkt Katastrophen und größere Gefahren- und Schadenslagen/sicherheitsrelevante Vorfälle i. Z. m. kritischen Infrastrukturen. Er wird an einen breiten Verteiler in Bund und Ländern gesteuert.

Diese Erkenntnisse werden regelmäßig auch in dem VS-NfD eingestuften Lagebericht Hybride Bedrohungen zusammengefasst. Der Lagebericht Hybride Bedrohungen wird den Bundesressorts und nachgeordneten Behörden sowie den Ländern über den Verfassungsschutzverbund in der Regel alle zwei Wochen zugestellt. Darüber hinaus erfolgt auf nationaler Ebene ein Informationsaustausch in der wöchentlich tagenden Task Force gegen Desinformation und weitere hybride Bedrohungen.

7. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in den Fragen 1 bis 4 erfragten Fälle zusammengetragen und im Sinne eines Lagebildes gebündelt werden, und wer hat darauf Zugriff oder wird wie darüber informiert?

   a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes?

   b) Plant die Bundesregierung künftig die Erstellung und Einrichtung eines entsprechenden Lagebildes?

   c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen für wen zusammengetragen werden?

Die Fragen 7 bis 7c werden gemeinsam beantwortet.

Polizeilich relevante Sachverhalte im Sinne der Fragen 1 bis 4 werden in den Zentralstellen des BKA zusammengetragen und phänomen- beziehungsweise tatmittelspezifisch gebündelt und ausgewertet. Es werden die Lagebilder Spionage (jährlich), Lagebilder Sabotage und Tatmittel Drohnen (beide quartalsweise) sowie perspektivisch das Lagebild Hybride Bedrohung (unter Federführung des BfV) erstellt und den Bedarfsträgern zur Verfügung gestellt.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) erstellt im Auftrag des BMI ein Lagebild zur Versorgungssituation mit kritischen Dienstleistungen (KRITIS-Lagebild). Es ist Bestandteil des „Gemeinsamen Lagebildes Bevölkerungsschutz“, welches vom Gemeinsamen Kompetenzzentrum Bevölkerungsschutz zweiwöchentlich aktualisiert und an einen Empfängerkreis in Bundesressorts und Ländern verteilt wird. Der Fokus liegt hierbei

jedoch nicht auf Vorfällen i. S. der Fragen 1 bis 4, sondern primär auf möglichen Einschränkungen bei der Versorgung mit kritischen Dienstleistungen. Quelle der Lageinformationen sind Bundesressorts (gemäß deren Zuständigkeit bezogen auf die KRITIS-Sektoren) und die Innenressorts der Länder.

Darüber hinaus wird auf die Antwort zu Frage 6 verwiesen.

8. Liegen der Bundesregierung Informationen darüber vor, in wie viel Prozent der in den Fragen 2 und 4 erfragten Fälle Betreiber von KRITIS überhaupt die Behörden informieren?

   a) Falls dies nicht immer der Fall ist, welche Maßnahmen plant die Bundesregierung, um ein zuverlässiges und verbindliches Meldesystem von KRITIS-Betreibern zu den Sicherheitsbehörden zu gewährleisten?

   b) An welche Stellen können sich Betreiber von KRITIS wenden, wenn sie die in den Fragen 2 und 4 erfragten Fälle beobachten?

   c) Falls es sich dabei um mehrere Stellen handelt, in welchem Maß und welchem zeitlichen Intervall und in welchem Format tauschen die beteiligten Behörden Informationen, die sie von Betreibern von KRITIS erhalten haben, aus?

   d) Plant die Bundesregierung die Einrichtung einer einheitlichen Meldestelle für Betreiber von KRITIS zur Meldung von in den Fragen 2 und 4 erfragten Fällen, und wenn ja, in welcher Bundesbehörde oder Stelle soll diese künftig angesiedelt werden?

Die Fragen 8 bis 8d werden gemeinsam beantwortet.

Erster Ansprechpartner sind die örtlichen Polizeidienststellen. Da bei Fällen von 2 und 4 meist Straftaten im Raum stehen, sind regelmäßig gefahrenabwehrende oder Strafverfolgungsmaßnahmen einzuleiten. Nach Auffassung der Bundesregierung ist hierdurch ein einheitlicher Meldeweg vorgegeben. Weitere Stellen werden sachverhaltsabhängig durch die Polizeidienststellen einbezogen. Betroffene können sich zusätzlich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie an Aufsichtsbehörden wenden. Das BSI unterrichtet gemäß § 8b Absatz 2 Nummer 4 BSIG unverzüglich Aufsichtsbehörden sowie das BBK bei meldepflichtigen KRITIS-Vorfällen in VS-NfD. Das BSI sensibilisiert KRITIS-Betreiber kontinuierlich bzgl. der Meldepflicht über verschiedene Kanäle.

Zudem sieht die CER-Richtlinie (Critical Entities Resilience Directive) vor, dass Betreiber von KRITIS künftig auch physische Vorfälle wie erhebliche Störungen oder Ausfälle an eine zentrale Stelle melden. Die CER-Richtlinie soll durch den derzeit erarbeiteten Entwurf eines KRITIS-Dachgesetzes in nationales Recht umgesetzt werden. Voraussichtlich soll der Gesetzentwurf Regelungen für ein Vorfallsmonitoring enthalten; das heißt, dass Betreiber von KRITIS Vorfälle dem BKK melden. Ziel dabei ist es, sektorübergreifend Interdependenzen zu erkennen und daraus Rückschlüsse zur Verbesserung eines künftigen KRITIS-Schutzes ziehen zu können.

Im aktuellen NIS2-Umsetzungssgesetz-Entwurf ist eine einheitliche Meldestelle aufgenommen worden, die Vorfälle nach KRITIS-DachG-Entwurf und NIS2-UmsuCG-Entwurf umfasst. Fälle nach 2 und 4 wären dann in die einheitliche Meldestelle integriert, wenn diese unter die in beiden Gesetzesentwürfen genannten Definitionen melderelevanter Vorfälle fallen.

9. Wie viele Fälle von Cyberangriffen, die nicht ausschließlich wirtschaftlich motiviert, sondern potenziell sicherheitsgefährdend sind, sind der Bundesregierung seit dem Jahr 2022 bekannt (bitte nach Jahren und Sektoren aufschlüsseln)?

10. Wie viele der in Frage 9 erfragten Fälle waren dergestalt erfolgreich, dass eine Beeinträchtigung deutscher oder europäischer Sicherheitsinteressen jedenfalls nicht ausgeschlossen werden kann (bitte nach Jahren aufschlüsseln)?

Die Fragen 9 und 10 werden gemeinsam beantwortet.

Umfangreiche Informationen zu Fällen von Cyberangriffen in Deutschland seit dem Jahr 2022 können den jährlich im Internet veröffentlichten IT-Sicherheits-Lageberichten des BSI („Die Lage der IT-Sicherheit in Deutschland 2022“, „Die Lage der IT-Sicherheit in Deutschland 2023“, „Die Lage der IT-Sicherheit in Deutschland 2024“) sowie den jährlich im Internet veröffentlichten Bundeslagebildern Cybercrime 2022 bis 2024 des BKA entnommen werden.

Darüber hinaus wird auf den 5. Punkt der Vorbemerkung der Bundesregierung verwiesen.

11. Wie viele der in Frage 9 erfragten Fälle können eindeutig oder wahrscheinlich staatlich oder staatlich gelenkten Akteuren zugeordnet werden (bitte nach Jahren aufschlüsseln und nach konkreten Staaten und eindeutiger bzw. wahrscheinlicher Attribution differenzieren)?

Auf die Antwort zu den Fragen 9 und 10 wird verwiesen.

Darüber hinaus lassen sich aus dem aus der Analyse von Einzelsachverhalten basierenden Lagebild und Trendbeobachtung des BfV Aussagen des Branchenverbands Bitkom bestätigen. Dieser hat auf Grundlage einer durchgeführten Umfrage unter seinen Mitgliedern für 2024 unter anderem festgestellt, dass 20 Prozent der Unternehmen durch (versuchte) Cyberspionage durch ausländische Nachrichtendienste betroffen waren und dies nahezu einer Verdreifachung der vorjährigen Zahlen gleichkommt. Ferner verweist die Bundesregierung auf den aktuellen und vergangene Verfassungsschutzberichte, in welchen umfassende Ausführungen zu staatlichen bzw. staatlich gelenkten Cyberangriffen enthalten sind.

12. Welche Erkenntnisse liegen der Bundesregierung dazu vor, wie hoch die Dunkelziffer der in Frage 9 erfragten Fälle ist, also wie viele Fälle gar nicht bekannt werden?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor. Im Übrigen wird auf den 5. Punkt der Vorbemerkung der Bundesregierung verwiesen.

13. In wie vielen der in Frage 9 erfragten Fälle wurde ein Ermittlungsverfahren eingeleitet?

    a) In vielen dieser Fälle konnten tatverdächtige Personen ermittelt werden?

    b) In wie vielen dieser Fälle kam es zu einer Verurteilung?

c) In wie vielen der in den Fragen 13, 13a und 13b erfragten Fälle (bitte differenzieren) konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)?

Die Fragen 13 bis 13c werden gemeinsam beantwortet.

Die Bundesregierung verweist auf ihren 4. und 5. Punkt der Vorbemerkung.

14. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in den Fragen 9 bis 13 erfragten Fälle zusammengetragen und im Sinne eines Lagebildes gebündelt werden?

a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes, und inwieweit würde ein solches Lagebild nach Auffassung der Bundesregierung dazu beitragen, die in den Fragen 9 bis 13 erfragten Fälle besser aufzuklären und zukünftig verhindern zu können?

b) Plant die Bundesregierung die Einrichtung eines entsprechenden Lagebildes?

c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen zusammengetragen werden?

d) Bei welchen Stellen bei der Bundesregierung oder den Landesregierungen liegen Informationen oder gar partielle Lagebilder über die in den Fragen 9 bis 13 erfragten Fälle vor?

Die Fragen 14 bis 14d werden gemeinsam beantwortet.

Das auf Bundesebene federführende Referat für hybride Bedrohungen einschließlich Desinformation im BMI sammelt systematisch aktuelle Fälle hybrider Bedrohungen im Cyberraum und stellt diese in dem VS-NfD eingestuften Lagebericht Hybride Bedrohungen regelmäßig zusammen. Der Lagebericht Hybride Bedrohungen wird den Bundesressorts und nachgeordneten Behörden sowie den Ländern über den Verfassungsschutzverbund in der Regel alle zwei Wochen zugestellt. Darüber hinaus erfolgt auf nationaler Ebene ein Informationsaustausch in der wöchentlich tagenden Task Force gegen Desinformation und weitere hybride Bedrohungen.

Das BKA veröffentlicht das jährliche Lagebild zu Spionage mit Cyberspionage und Staatsterrorismus, Proliferation (VS-NfD) mit Aussagen und statistischer Erfassung zu Cyberspionage und fungiert als polizeiliche Zentralstelle in diesem Phänomenbereich.

15. Welche Vorkehrungen trifft die Bundesregierung im Rahmen der Umsetzung der NIS-2-Richtlinie (zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit), um sicherzustellen, dass sämtliche, bei Betreibern von KRITIS vorliegenden, relevanten Informationen über die in den Fragen 9 bis 13 erfragten Fälle beim Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch allen anderen betroffenen Behörden vorliegen und Teil eines einheitlichen Lagebildes werden?

Der aktuelle NIS2-Umsetzungsgesetz-Entwurf sieht weiterhin – ähnlich zu den bereits heute in § 8b des BSI-Gesetzes verankerten Pflichten – Weiterleitungs- und Unterrichtungspflichten an Aufsichtsbehörden und zuständige Stellen vor.

16. Wie viele Fälle von Desinformation und Einflussnahme auf demokratische Willensbildungsbildungsprozesse in Deutschland seit dem Jahr 2022 sind der Bundesregierung bekannt, die von eindeutig oder wahrscheinlich staatlichen oder staatlich gelenkten Akteuren ausgegangen sind (bitte nach Jahren aufschlüsseln und nach konkreten Staaten und eindeutiger bzw. wahrscheinlicher Attribution differenzieren)?

    a) Wie viele dieser Fälle sind nach Kenntnisstand und Auffassung der Bundesregierung nach deutschem Recht strafbar?

    b) In wie vielen dieser strafbaren Fälle wurde ein Ermittlungsverfahren eingeleitet und konnten Tatverdächtige ermittelt werden?

    c) In wie vielen dieser Fälle kam es zu einer Verurteilung?

    d) In wie vielen Fällen konnten Bezüge zu ausländischen Nachrichtendiensten und bzw. oder Auftraggebern bzw. Hintermännern festgestellt werden (bitte nach Ländern aufschlüsseln)

Die Fragen 16 bis 16d werden gemeinsam beantwortet.

Es wird auf die Antwort der Bundesregierung zu den Fragen 6 bis 12 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/13880 verwiesen.

    e) Wie viele Fälle standen im Zusammenhang mit den Bundestagswahlen 2025?

Die Bundestagswahl 2025 wurde nicht von ausländischen Akteuren manipuliert. Es gibt keinen Zweifel an der Integrität der Wahl.

Im Vorfeld der Bundestagswahl gab es Versuche der ausländischen Einflussnahme im Informationsraum. Diese zielten v. a. darauf ab, das Vertrauen in den demokratischen Wahlprozess zu erschüttern und das Wahlverhalten der Wahlberechtigten zu beeinflussen.

Insbesondere Russland führte mit großer Wahrscheinlichkeit mehrere verdeckte Einflussnahmeoperationen und Kampagnen im Informationsraum durch, um die Wahl zu seinen Gunsten zu beeinflussen. Diese Einflussnahmeversuche generierten in der Regel aber relativ geringe Reichweiten.

Darüber hinaus verweist die Bundesregierung auf ihren 4. Punkt der Vorbemerkung.

17. Gibt es eine einheitliche Stelle bei der Bundesregierung, bei der sämtliche Informationen über die in Frage 16 erfragten Fälle im Sinne eines Lagebildes gebündelt vorliegen?

    a) Wenn nein, wie bewertet die Bundesregierung das Fehlen eines entsprechenden Lagebildes, und inwieweit würde ein solches Lagebild nach Auffassung der Bundesregierung dazu beitragen, die in Frage 16 erfragten Fälle besser aufzuklären und gezielte Gegenmaßnahmen einleiten zu können?

    b) Plant die Bundesregierung die Einrichtung eines entsprechenden Lagebildes?

    c) Wenn ja, bei welcher Stelle soll ein solches Lagebild vorliegen, welche – auch nichtstaatlichen – Stellen sollen zur Informationsübermittlung verpflichtet oder ermutigt werden, und in welchem zeitlichen Intervall (täglich bzw. wöchentlich bzw. monatlich) sollen dort relevante Informationen zusammengetragen werden?

Die Fragen 17 bis 17c werden gemeinsam beantwortet.

Das auf Bundesebene federführende Referat für hybride Bedrohungen einschließlich Desinformation im BMI sammelt systematisch aktuelle Fälle ausländischer Desinformation und stellt diese in dem VS-NfD eingestuften Lagebericht Hybride Bedrohungen regelmäßig zusammen. Der Lagebericht Hybride Bedrohungen wird den Bundesressorts und nachgeordneten Behörden sowie den Ländern über den Verfassungsschutzverbund in der Regel alle zwei Wochen zugestellt. Darüber hinaus erfolgt auf nationaler Ebene ein Informationsaustausch in der wöchentlich tagenden Task Force gegen Desinformation und weitere hybride Bedrohungen. Unter dem Dach der AG Hybrid arbeitet zudem die seit 2018 bestehende Expertengruppe „Medien- und Informationsarbeit zu Desinformation hybriden Bedrohungslagen“ (kurz „EG Desinformation“) unter Leitung des Auswärtigen Amtes und des Bundespresseamtes.

Die Projektgruppe „Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation“ (ZEAM) im BMI befindet sich seit 1. Juni 2024 im Aufbau. Im Rahmen ihres Auftrags nimmt sie die Vorgehensweise, die Verbreitungswege, sowie die Mechanismen ausländischer Einflussnahme durch Informationsmanipulation in sozialen Netzwerken und im Internet in den Blick, um diese besser verstehen und möglichst früh erkennen zu können.

Das Auswärtige Amt hat den gesetzlichen Auftrag, die Interessen der Bundesrepublik Deutschland im Ausland zu vertreten sowie die Bundesregierung über Verhältnisse und Entwicklungen im Ausland zu unterrichten (GAD § 1 Absatz 2). Diesem Auftrag kommt das Auswärtige Amt durch die Erstellung von Lagebildern und Berichterstattung über die Entwicklungen im Ausland nach. Im Rahmen des Auftrags des GAD beobachtet das Auswärtige Amt auch öffentliche Debatten in den sozialen Medien. Hierzu gehört auch die anlassbezogene Analyse von möglichen inauthentischen Verzerrungen und der Informationsmanipulation. Diese Analyseerkenntnisse fließen als Teil von Lagebildern in die außenpolitische Entscheidungsfindungen ein.

d) Welche Maßnahmen hat die Bundesregierung ergriffen, um den Schaden durch Desinformation einzugrenzen, und was gedenkt sie darüber hinaus an Maßnahmen zu ergreifen, und inwiefern prüft sie dabei den Einsatz auch digitaler Technologien (ggf. welcher konkret)?

Die Bundesregierung nimmt die Bedrohung durch ausländische Einflussnahme und Manipulation im Informationsraum sehr ernst und tritt ihr entschlossen entgegen. Die zuständigen Behörden führen im Rahmen ihrer fachlichen Zuständigkeiten und nach Maßgabe der gesetzlichen Befugnisse eine Vielzahl an Maßnahmen der Prävention, Detektion und Reaktion durch.

Zudem arbeitet die Bundesregierung im Bereich des Umgangs mit Desinformation mit zivilgesellschaftlichen Organisationen zusammen. So hat das BMI u. a. mit der Bertelsmann Stiftung im Projekt „Forum gegen Fakes – Gemeinsam für eine starke Demokratie“ kooperiert, das eine bundesweite Debatte zum Umgang mit Desinformation angestoßen hat. Überdies hat das BMI das Projekt „Jahr der Nachricht 2024“ der UseTheNews gGmbH gefördert, welches zur Stärkung der Medien- und Nachrichtenkompetenz, gerade der jüngeren Bürgerinnen und Bürger, sowie der gesellschaftlichen Resilienz gegen Desinformation beigetragen hat.

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

e) In welchem formellen und informellen Rahmen tauscht sich die Bundesregierung mit anderen betroffenen Staaten, insbesondere im europäischen, transatlantischen und indopazifischen Raum, dazu aus?

Es wird auf die Antwort der Bundesregierung zu Frage 41 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/12872 verwiesen.

18. Welche Maßnahmen trifft die Bundesregierung, um die Bevölkerung über das Ausmaß und die Gefahren ausländischer, insbesondere russischer und chinesischer, nachrichtendienstlicher Tätigkeiten auf dem Gebiet des Bundesrepublik Deutschland zu unterrichten und ihre Kompetenzen zum Umgang damit zu stärken?

Die Bundesregierung misst der Aufklärung über die Gefahren von Aktivitäten gegnerischer Nachrichtendienste in Deutschland eine hohe Bedeutung bei. Zur Sensibilisierung und Information ergreift sie eine Vielzahl an Maßnahmen und nutzt dabei Publikationen, digitale Formate, Präventionsangebote und auch direkte Zusammenarbeit. Beispielhaft sei hier als ein zentrales Instrument der jährlich vom BMI herausgegebene Verfassungsschutzbericht genannt. Der Bericht enthält u. a. umfassende Informationen zu Aktivitäten fremder Staaten in Deutschland. Darüber hinaus veröffentlicht das BfV regelmäßig Fachpublikationen und Informationsbroschüren zum Thema.

Die Bundesregierung prüft laufend und in Abhängigkeit eines Ereignisses – auch im Sinne der Prävention sowie des Aufbaus von gesamtstaatlicher und gesellschaftlicher Resilienz – geeignete Berichtsformen. Das BMI stellt mehrsprachig umfangreiche Informationsmaterialien zur Sensibilisierung der Öffentlichkeit für hybride Bedrohungen einschließlich Desinformation bereit, u. a. abrufbar unter www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html sowie www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html.

a) Plant die Bundesregierung, etwa im Zuge der Einrichtung eines nationalen Sicherheitsrats, eine grundlegende Neuordnung des Informationsflusses zwischen den Landes- und Bundesbehörden mit Blick auf Sabotage, Spionage und Desinformation?

b) Wenn ja, welche?

Die Fragen 18a und 18b werden gemeinsam beantwortet.

Die Bundesregierung arbeitet beständig an einer weiteren Verbesserung des Informationsflusses zwischen den Behörden und den föderalen Ebenen. Der geplante Nationale Sicherheitsrat soll dazu einen Beitrag leisten.

c) Wenn ja, ist der Bundesregierung bekannt, welche Auffassung die Innenministerkonferenz (IMK) zu dieser Frage vertritt, und welche Rolle sollte die IMK nach Auffassung der Bundesregierung dabei spielen?

Das auf Bundesebene federführende Referat für hybride Bedrohungen einschließlich Desinformation im BMI leitet die auf Beschluss der IMK vom Dezember 2021 gegründete Bund-Länder-offene Arbeitsgruppe Hybride Bedrohungen (BLoAG Hybrid). In der BloAG Hybrid sind neben Bundesressorts und den Sicherheitsbehörden des Bundes die ressortübergreifend und koordinierend federführenden Ansprechstellen der Länder zu hybriden Bedrohungen (Single Points of Contact – SPOC) sowie die kommunalen Spitzenverbände, der Verband der kommunalen Unternehmen (VkU) sowie die LAG Cybersicherheit vertreten. Die BloAG Hybrid kann dadurch wesentlich zur Informationsweiter-

gabe und Sensibilisierung der Bevölkerung in den Ländern und Kommunen beitragen. Die IMK hatte im Dezember 2023 die Einrichtung der SPOC als feste Strukturen zur Bekämpfung hybrider Bedrohungen einschließlich Desinformation empfohlen, über die der Informationsaustausch zwischen Bund und Ländern in der BloAG Hybrid erfolgen soll. Die Ministerpräsidentenkonferenz (MPK) verpflichtete sich im Juni 2024 daraufhin, bis September 2024 zentrale Koordinierungs- und Ansprechstellen (Single Points of Contact – SPOC) für das Thema hybride Bedrohungen und Desinformation einzurichten, die im Bund und im Land jeweils federführend sind.

19. Sieht die Bundesregierung den Bedarf, eigene Bemühungen im weiten Feld der „Strategischen Kommunikation“ auszubauen und zu verbessern, und wenn ja, wo genau, und mit welchem Ziel und welchen Maßnahmen (bitte konkret aufschlüsseln)?

Im Bereich der strategischen Kommunikation haben sich ressortübergreifend eingespielte Strukturen entwickelt, auf deren Grundlage die Bundesregierung die Öffentlichkeit informiert und sensibilisiert. Von besonderer Bedeutung bleiben hierbei die Prävention und der Aufbau von gesamtstaatlicher und gesellschaftlicher Resilienz.

Die Bundesregierung kommuniziert stets proaktiv, transparent und faktenbasiert, auch um die gesellschaftliche Resilienz gegen hybride Bedrohungen weiter zu stärken. Dabei setzt die Bundesregierung Desinformation ganz konkret die eigene umfassende und sachliche Information der Öffentlichkeit entgegen.

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