Deutscher Bundestag **Drucksache 20/4267**

20. Wahlperiode 02.11.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/3915 –

Schutz kritischer Infrastrukturen in Deutschland

Vorbemerkung der Fragesteller

Die Fragesteller stellen fest, dass der verbrecherische Angriffskrieg Putins gegen die Ukraine nicht nur die militärische und außenpolitische Sicherheitslage Deutschlands grundlegend verändert, sondern auch tiefgreifende Auswirkungen auf die innere Sicherheit hat. Dabei sind auch gezielte Sabotageangriffe und Spionageaktivitäten, insbesondere gegen Sicherheitsbehörden, kritische Infrastrukturen sowie rüstungsnahe Wirtschaftsunternehmen, einzukalkulieren. Die Sicherheitsbehörden gehen vor diesem Hintergrund von einer erhöhten Bedrohung aus. Gerade der wirksame Schutz kritischer Infrastrukturen aus den Sektoren Energie, Ernährung und Landwirtschaft, Gesundheit, Soziales, Informationstechnik und Telekommunikation, Medien und Kultur, Staat und Verwaltung, Transport und Verkehr ist eine der wichtigsten Kernaufgaben staatlicher, unternehmerischer und bürgerschaftlicher Sicherheitsvorsorge.

Das Bundeskriminalamt (BKA) warnte erst kürzlich in einem öffentlich gewordenen internen Papier vor Angriffen von sogenannten Aktivisten gegen Kernkraftwerke, Gaspipelines und auf den gesamten Schwerlastverkehr (vgl. https://www.tagesspiegel.de/politik/debatte-um-fossile-energiequellen-bundeskriminalamt-warnt-vor-gefahr-linksextremer-attacken-8637625.html). Demnach befürchtet das BKA, dass die „linke Szene“ aus „Themenfeldern, wie beispielsweise Antimilitarismus, Antikapitalismus, Klimaschutz und Nachhaltigkeit“, „Besetzungs- und Blockadeaktionen sowie Sachbeschädigungen oder Brandstiftungen gegen den Energiesektor“ planen könnten. Es sei von einer „abstrakten Gefährdung der Energie-Infrastruktur auszugehen“, die bei weiterer Verschärfung der Lage „neben zunehmenden und mitunter emotionalisierten Demonstrations- und Protestversammlungen“ auch zu „Straftaten zum Nachteil der Energie-Infrastruktur sowie hiermit assoziierten Institutionen und Entscheidungsträgern“ führen könnte.

Laut „Redaktionsnetzwerk Deutschland“ hat eine führende deutsche Vertreterin von Fridays for Future bereits im Sommer 2022 öffentlich mit entsprechenden Gedanken gespielt (vgl. https://www.rnd.de/politik/klimaaktivistin-luisa-neubauer-pipeline-in-die-luft-sprengen-JZLNOWO7HVBELCU7OGJEZZYYAU.html).

Mit den mutmaßlich von staatlichen Akteuren verübten Sabotageakten auf die beiden Gaspipelines Nord Stream 1 und 2 am 27. September 2022 ist nunmehr eine neue Bedrohungsstufe erreicht. Der Vorfall zeigt, wie verwundbar kriti-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 2. November 2022 übermittelt.

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

sche Infrastruktureinrichtungen sind und dass womöglich gezielt zivile kritische Infrastrukturen außerhalb der Ukraine angegriffen werden. Der Inspekteur der Marine teilte in der Welt vom 26. September 2022 auf Seite 2 seine Erkenntnisse über „russische Unter- und Überwassereinheiten“, die sich „über längere Zeit im Bereich dieser Kabel aufhalten“, und warnt vor den Gefahren gegenüber den kritischen Infrastrukturen in Ostsee und Atlantik.

Die deutsche Öffentlichkeit hat daher ein besonderes Informationsinteresse daran, von der Bundesregierung zu erfahren, welche konkreten oder abstrakten Hinweise der Bundesregierung zu potenziellen Anschlagsbedrohungen auf kritische Infrastruktureinrichtungen vorliegen und welche Gegenmaßnahmen sie unternimmt, um dieser Bedrohungslage entgegenzuwirken.

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu dem Schluss gekommen, dass eine Auskunft zu den Fragen 1 bis 3 in Teilen aus Gründen des Staatswohls nicht – auch nicht in eingestufter Form – erteilt werden kann. Die erbetene Auskunft unterliegt den Restriktionen der „Third-Party-Rule“, die den internationalen Austausch von Informationen der Nachrichtendienste betrifft. Die Bedeutung der „Third Party Rule“ für die internationale nachrichtendienstliche Zusammenarbeit hat das Bundesverfassungsgericht in seinem Beschluss 2BvE 2/15 vom 13. Oktober 2016 (Rz. 162-166) gewürdigt.

Liegen solche Informationen vor, sind diese evident geheimhaltungsbedürftig, weil sie sicherheitsrelevante Erkenntnisse beinhalten, die unter der Maßgabe der vertraulichen Behandlung von ausländischen Nachrichtendiensten an die deutschen Nachrichtendienste weitergleitet wurden. Ein Bekanntwerden von Informationen, die nach den Regeln der „Third-Party-Rule“ erlangt wurden, würde als Störung der wechselseitigen Vertrauensgrundlage gewertet werden und hätte eine schwere Beeinträchtigung der Teilhabe der Nachrichtendienste des Bundes am internationalen Erkenntnisaustausch zur Folge. Eine mögliche Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit der Nachrichtendienste des Bundes mit ausländischen Nachrichtendiensten haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland.

Ein Bekanntwerden der Informationen würde zudem die weitere Aufklärung geheimdienstlicher Aktivitäten in und gegen die Bundesrepublik Deutschland erheblich erschweren. Die erbetenen Informationen berühren somit derart schutzbedürftige Geheimhaltungsinteressen, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt und das Fragerecht der Abgeordneten ausnahmsweise gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen muss.

Selbst eine VS-Einstufung und Hinterlegung der angefragten Informationen bei der Geheimschutzstelle des Deutschen Bundestages würde im vorliegenden Fall nicht ausreichen, um der besonderen Sensibilität der angeforderten Informationen für die Aufgabenerfüllung der Nachrichtendienste des Bundes ausreichend Rechnung zu tragen.

1. Wie hat die Bundesregierung die Bedrohungslage für kritische Infrastruktureinrichtungen, insbesondere auch solche zur Sicherstellung der Energieversorgung oder Untersee-Telekommunikationskabel in der Ostsee, durch Sabotageakte, Anschläge oder Cyberangriffe unmittelbar vor Beginn des verbrecherischen Angriffskrieges Putins gegen die Ukraine am 24. Februar 2022 bewertet, und inwiefern hat sich die Bewertung danach geändert?

Von einer Befähigung der russischen Nachrichtendienste zu komplexen Operationen mit erheblicher Wirkung auch im westlichen Ausland war und ist auszugehen. Gleichwohl wurden kritische Infrastrukturen bzw. deren Beeinträchtigung nicht als prioritäres Ziel der russischen Seite angesehen. Hierbei sind insbesondere die einzukalkulierenden erheblichen außenpolitischen Konsequenzen entsprechender Angriffe zu beachten.

Die Bundesregierung betrachtet grundsätzlich alle kritischen Infrastrukturen einschließlich ihrer Peripherietechnik als abstrakt gefährdet.

Seit dem Beginn des russischen Angriffskrieges gegen die Ukraine geht die Bundesregierung von einer erhöhten Bedrohungslage für Kritische Infrastruktur in Deutschland aus. Auch künftig sind weitere (hybride) Angriffe gegen ebendiese Einrichtungen in Betracht zu ziehen.

Seit Beginn des russischen Angriffskrieges gegen die Ukraine besteht eine erhöhte Gefährdungslage für Deutschland durch Cyberangriffe. Es wurden noch keine breit angelegten Kampagnen gegen kritische Infrastrukturen in Deutschland beobachtet.

Weitere Informationen im Sinne der Fragestellung kann die die Bundesregierung nach sorgfältiger Abwägung nicht offen übermitteln. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Frage würde Informationen zu Arbeitsmethoden, Vorgehensweise sowie Einzelheiten der nachrichtendienstlichen Erkenntnislage des Bundesamtes für Verfassungsschutz einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Eine Veröffentlichung würde zu einer wesentlichen Schwächung der dem Bundesamt für Verfassungsschutz (BfV) zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die jeweilige Auftragserfüllung erhebliche Nachteile zur Folge haben. Die Veröffentlichung kann daher für die Interessen der Bundesrepublik schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.*

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

2. Hat die Bundesregierung nach Beginn des Krieges gegen die Ukraine von Sicherheitsbehörden des Bundes, der Länder oder ausländischer Staaten Hinweise konkreter oder abstrakter Art zu Sabotageakten, Anschlägen oder Cyberangriffen auf Gaspipelines, Untersee-Telekommunikationskabel in der Ostsee und andere kritische Infrastruktureinrichtungen erhalten, und inwiefern konnten diese Hinweise genutzt werden, um potenzielle Gefahrenabwehrmaßnahmen anzupassen?

Der Bundesnachrichtendienst (BND) hat gemäß § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) den Auftrag, Erkenntnisse über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundes-

* 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.

republik Deutschland sind, zu sammeln und auszuwerten. Der BND unterrichtet in diesem Rahmen selbstverständlich auch die Bundesregierung. Darüber hinaus wird auf die Antwort der Bundesregierung auf die Schriftliche Frage des Abgeordneten Jürgen Hardt, Arbeits-Nr. 9/538, die am 13. Oktober versandt wurde, verwiesen.

Informationen des BfV, die auf konkrete Gefährdungen im Sinne der Fragestellungen schließen lassen, werden im Rahmen der gesetzlichen Übermittlungsvorschriften an die zuständigen Stellen weitergegeben.

Darüber hinaus unterrichtet und sensibilisiert das BfV im Rahmen seines Aufklärungsauftrages (vgl. § 16 des Bundesverfassungsschutzgesetzes – BVerfSchG) auch andere Stellen der Politik, Verwaltung, Wirtschaft und Wissenschaft, um sie in die Lage zu versetzen, ihre individuelle Resilienz gegenüber Angriffen zu stärken. Beispielsweise werden im Verfassungsschutzverbund bei potentiell betroffenen Unternehmen Sensibilisierungsmaßnahmen durchgeführt und die zuständigen Behörden im Nationalen Cyber-Abwehrzentrum informiert.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

3. Hat die Bundesregierung nach Beginn des Krieges gegen die Ukraine Hinweise konkreter oder abstrakter Art zu Sabotageakten, Anschlägen oder Cyberangriffen auf für den Kohle-, Flüssiggas-, Militär- oder Getreidetransport zu nutzenden bundeseigenen und nicht bundeseigenen Schienenstrecken erhalten, und inwiefern konnten diese Hinweise genutzt werden, um potenzielle Gefahrenabwehrmaßnahmen anzupassen?

Der Bundesregierung liegen keine Hinweise zu konkreten Gefährdungen im Sinne der Fragestellung vor.

Darüber hinaus wird auf die Antwort zu Frage 2 verwiesen.

4. Wie erklärt die Bundesregierung, dass die Bundesministerin des Innern und für Heimat, Nancy Faeser, im August 2022 öffentlich vor Attacken auf die Energieinfrastruktur in Deutschland warnt (vgl. Berichterstattung auf https://www.bild.de/bild-plus/politik/inland/politik/faeser-muessen-gegen-moegliche-attacken-auf-gas-terminals-geruestet-sein-80997976.bild.html), auf parlamentarische Nachfrage aber mitteilen lässt, dass die Bundesregierung keine konkreten Informationen zu geplanten Straftaten gegen die Energieinfrastruktur habe (siehe Antwort der Bundesregierung auf die Schriftliche Frage 74 auf Bundestagsdrucksache 20/3429)?

Seit dem Beginn des russischen Angriffskrieges gegen die Ukraine geht die Bundesregierung von einer erhöhten Bedrohungslage für kritische Infrastruktur in Deutschland aus, die auf eine ohnehin schon angespannte Gesamtbedrohungslage trifft. Die Sicherheitsbehörden gehen davon aus, dass grundsätzlich alle Anlagen der kritischen Infrastruktur ein potenzielles Ziel von Angriffen sein können.

Ferner wird auf die Antwort zu Frage 3 verwiesen.

5. Sind der Bundesregierung die Aktivitäten vorgeblicher Forschungsschiffe aus Russland bekannt (vgl. Berichterstattung auf https://www.t-online.de/nachrichten/deutschland/aussenpolitik/id_100059064/nord-stream-lecks-europas-achillesfersen-so-angreifbar-ist-unsere-infrastruktur.html), die immer wieder vor der Westküste Irlands im Umfeld transatlantischer Kommunikationsinfrastruktur gesichtet werden, und gibt es nach Kenntnis solche Aktivitäten auch in der Ost- und Nordsee vor deutschen Küsten?

Die Antwort zu Frage 5 kann nicht offen erfolgen. Die Einstufung der Antwort auf die Frage als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ ist im vorliegenden Fall im Hinblick auf das Staatswohl erforderlich.

Nach der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Frage würde Informationen zur Methodik und zu der Erkenntnislage des Bundesnachrichtendienstes einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Eine solche Veröffentlichung von Einzelheiten ist daher geeignet, zu einer wesentlichen Verschlechterung der dem BND zur Verfügung stehenden Möglichkeiten der Informationsgewinnung zu führen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.*

6. Welche Aufklärungsergebnisse, Informationen und Erkenntnisse lagen der Bundesregierung zu den mutmaßlichen Sabotageakten auf die Gaspipelines Nord Stream 1 und 2 am 27. September 2022 vor?

Zu diesem Zeitpunkt war bekannt, dass es plötzlich zu drei Lecks an den Röhren von Nord Stream I und II kam und starker Gasaustritt mit entsprechendem Druckabfall in den Röhren zu verzeichnen war.

Dazu gab es aufgrund von seismischen Aktivitäten erste Hinweise auf eine starke Unterwasserexplosion, die auf eine nicht-natürliche Ursache hindeuteten.

Es wird darüber hinaus auf die Antwort der Bundesregierung auf die Schriftliche Frage des Abgeordneten Jürgen Hardt, Arbeits-Nr. 9/538, die am 13. Oktober versandt wurde, verwiesen.

Am 10. Oktober 2022 hat der Generalbundesanwalt beim Bundesgerichtshof ein Ermittlungsverfahren gegen Unbekannt wegen Verdachts des vorsätzlichen Herbeiführens einer Sprengstoffexplosion in Tateinheit mit verfassungsfeindlicher Sabotage gemäß § 308 Absatz 1, § 88 Absatz 1 Nummer 3, § 52 StGB eingeleitet.

* 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.

7. Welche Erkenntnisse hat die Bundesregierung vor dem Hintergrund der in der Vorbemerkung der Fragesteller dargestellten Aussagen des Inspekteurs der Marine über Flottenbewegungen der russischen Marine (vgl. Ausgabe der Welt vom 26. September 2022, S. 2)?

Auf die Antwort zu Frage 5 wird verwiesen.

8. Welche Bedrohung leitet die Bundesregierung für Angriffe auf kritische Infrastrukturen ab?

Sabotageaktivitäten gegen kritische Infrastrukturen, beispielsweise mit Cyberangriffen oder durch physische Einwirkung, stellen eine ernstzunehmende und einzukalkulierende Gefahr dar.

Darüber hinaus wird auf die Antwort zu Frage 1 verwiesen.

9. Welche (örtlich begrenzten) Vorsorgemaßnahmen sieht die Bundesregierung vor?

Grundsätzlich sind in Deutschland die Betreiber kritischer Infrastrukturen verantwortlich für den Schutz vor Sabotagehandlungen. Hierzu bestehen verschiedene rechtliche Vorgaben. Zudem finden sich in Publikationen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) Anleitungen zur Sicherung der Anlagen.

Die zuständigen Behörden informieren und sensibilisieren betroffene Stellen über die erhöhte Gefährdungslage fortlaufend und stellen umfangreiche Handlungsempfehlungen zur Verfügung.

10. Wenn keine Aufklärungsergebnisse, Informationen oder Erkenntnisse vorlagen: Welche Maßnahmen plant die Bundesregierung, um ein valides Lagebild zu generieren und eine sachgerechte Bedrohungslage bewerten zu können?

Im Auftrag der Bundesregierung erfolgt auf regelmäßiger Basis mit den relevanten Akteuren aus den Bereichen Sicherheit und Verteidigung eine Abstimmung zu relevanten Sicherheitsthemen, um ein umfassendes, gemeinsames Lagebild zu entwickeln und so im Dialog die notwendigen Handlungs- und Informationsbedarfe der operativen Ebene zu identifizieren, die dann durch die zuständigen Sicherheitsbehörden in eigener Zuständigkeit umgesetzt werden können.

Das BfV steht im regelmäßigen Austausch mit nationalen und internationalen Partnerdiensten, um Hinweisen auf mögliche Bedrohungen nachgehen und bei Bedarf eine Anpassung der hiesigen Gefährdungsbewertung vornehmen zu können.

Sofern hier Informationen auf eine konkrete Gefährdung von kritischen Infrastrukturen bekannt werden, werden diese umgehend bearbeitet und mit den zuständigen Behörden geteilt. Die aufgeführten Erkenntnisse fließen regelmäßig auch in öffentlich zugängliche Lagebilder des Bundesamtes für Verfassungsschutz sowie den jährlich erscheinenden Verfassungsschutzbericht ein.

11. Welche Rolle wird die Deutsche Marine konkret in Kooperation insbesondere mit den neuen NATO-Partnern Schweden und Finnland bei der Sicherung Übersee wie Untersee im Ostseeraum übernehmen, und welche Fähigkeiten sind hierfür erforderlich bzw. müssen noch geschaffen werden?

Mit Beginn des Russischen Angriffskriegs gegen die Ukraine hat die Marine ihre Präsenz in der Ostsee mit der Aktivität „BALTIC GUARD“ signifikant erhöht und setzt damit die im Rahmen der NATO vereinbarten erhöhten Wachsamkeitsaktivitäten, sogenannte enhanced Vigilance Activities um. Darüber hinaus ist die Zusammenarbeit im Ostseeraum auf maritimer Ebene durch eine sehr enge Zusammenarbeit der Befehlshaber der Flotten gekennzeichnet. Im Rahmen der Baltic Commanders Conference, in der die Ostsee-Anrainerstaaten zusammenkommen, findet dazu ein regelmäßiger Austausch statt.

In Bezug auf Finnland und Schweden erfolgen Kooperationen anlass- oder projektbezogen, auch im Rahmen von gemeinsamen Übungen. Zusätzlich erfolgen bilaterale Absprachen mit Schwerpunktsetzung auf regionale Zusammenarbeit.

12. Inwieweit gibt es Verabredungen oder Pläne der NATO, Einrichtungen der kritischen Infrastruktur, die nicht im Hoheitsgebiet eines Mitgliedstaates stehen oder im Eigentum eines Angehörigen eines Mitgliedstaates sind, vor Angriffen zu schützen und erforderlichenfalls zu verteidigen, und wie ist die Haltung der Bundesregierung hierzu?

Die NATO-Verteidigungsministerinnen und -minister haben bei ihrem Treffen am 12./13. Oktober 2022 vereinbart, den Schutz von Infrastruktur Untersee und im Energiebereich zu verstärken. Nationale kritische Infrastrukturen bzw. verteidigungswichtige Infrastruktur sind auch Gegenstand von NATO Planungen.

13. Welche Maßnahmen hat die Bundesregierung nach Beginn des Krieges gegen die Ukraine am 24. Februar 2022 wann genau konkret unternommen, um kritische Infrastruktureinrichtungen, insbesondere solche zur Sicherstellung der Energieversorgung oder Untersee-Telekommunikationskabel in der Ostsee, vor Sabotageakten, Anschlägen und Cyberangriffen zu schützen (bitte jeweils nach Datum, Art der Maßnahme und Begründung aufschlüsseln)?

Grundsätzlich sind in Deutschland die Betreiber kritischer Infrastrukturen für deren Schutz verantwortlich. Ihnen obliegt bei abstrakten Gefährdungen kritischer Infrastrukturen insoweit das Treffen erforderlicher Maßnahmen. Erst bei konkreten Gefährdungen von kritischen Infrastrukturen sind die Sicherheitsbehörden in Bund und Ländern zuständig.

Darüber hinaus wirkt die Bundespolizei im Rahmen ihrer Aufgabenwahrnehmung in Nord- und Ostsee beim Schutz von kritischen Infrastrukturen mit, indem sie mobile und stationäre maritime Infrastrukturen in die operative Planung ihrer Präsenzmaßnahmen auf See mit einbezieht. Zudem hat die Bundesregierung in dem besagten Zeitraum entsprechende Sensibilisierungsmaßnahmen der Betreiber kritischen Infrastrukturen durchgeführt.

a) Welche oberste Bundesbehörde und welche Behörde ist in der Bundesregierung federführend für die Aufklärung der Hintergründe zu den mutmaßlichen Sabotageakten auf Nord Stream 1 und 2 am 27. September 2022 zuständig?

Die Zuständigkeit für die Ermittlungen liegt beim Generalbundesanwalt (GBA). Der GBA ist eine Behörde im Geschäftsbereich des Bundesministeriums der Justiz (BMJ).

b) Welche oberste Bundesbehörde und welche Behörde ist in der Bundesrepublik Deutschland federführend für die Sicherheit von Untersee-Telekommunikationskabeln zuständig?

Der Schutz der Telekommunikationsinfrastruktur obliegt den Betreibern. Diese müssen angemessene technische und organisatorische Maßnahmen zum Schutz gegen Störungen und zur Beherrschung von Sicherheitsrisiken ergreifen.

Diese Vorgaben erstrecken sich auch auf Unterseekabel, soweit diese dem nationalen Recht unterliegen.

c) Verfügt die Bundesregierung über ein aktuelles Gesamtmonitoring aller Untersee-Telekommunikationskabel im Hoheitsgebiet der Bundesrepublik Deutschland?

Die Bundesregierung verfügt nicht über ein aktuelles Gesamtmonitoring aller Untersee-Telekommunikationskabel im Hoheitsgebiet der Bundesrepublik Deutschland.

d) Über welche Kapazitäten (wie z. B. Unterwasserdrohnen, Unterwasserroboter etc.) verfügt die federführend zuständige Behörde zum Schutz der Untersee-Telekommunikationskabel?

Auf die Antwort zu Frage 13b wird verwiesen.

14. Welche Maßnahmen zur Stärkung der Krisenvorsorge hat die Bundesregierung konkret unternommen, wie dies Bundesinnenministerin Nancy Faeser im April 2022 gefordert hat (vgl. Berichterstattung auf https://www.tagesschau.de/inland/zivilschutz-staerkung-faeser-101.html)?

15. Welche Maßnahmen zur Stärkung des Bevölkerungsschutzes und der Katastrophenhilfe hat die Bundesregierung konkret unternommen, und wie passt dies mit den geplanten Etatkürzungen für den Bundeshaushalt 2023 in diesem Bereich zusammen?

Die Fragen 14 und 15 werden gemeinsam beantwortet.

Das BMI formuliert mit dem neu vorgestellten Programm „Unser Land gegen Krisen und Klimafolgen wappnen − Neustart im Bevölkerungsschutz“ zentrale Leitlinien, um die Widerstandsfähigkeit der Gesellschaft durch Vorbereitungs- und Vorsorgemaßnahmen zu erhöhen, die Warnung zu verbessern und ein effizienteres Krisenmanagement von Katastrophen- und Zivilschutzbehörden, den Feuerwehren und wichtigen Hilfsorganisationen zu erreichen.

Das Programm enthält konkrete Ansätze und Maßnahmen, um Krisenereignissen, wie Extremwetter, Hochwasser oder Waldbränden künftig effektiver begegnen zu können. Hierzu gehört beispielsweise die gemeinsam mit den Ländern Anfang Juni vorgenommene Schaffung des Gemeinsamen Kompetenzzentrums Bevölkerungsschutz (GeKoB) beim BBK.

Ziel des Kompetenzzentrums ist die von Bund und Ländern partnerschaftlich getragene Errichtung und Etablierung einer dauerhaften und strukturiert organisierten Kooperationsplattform für den Bevölkerungsschutz und die Unterstützung des ressortübergreifenden Risiko- und Krisenmanagements. Gemeinsame Lagebewertungen, abgestimmte Risikoanalysen und ein gemeinsames Ressourcenmanagement werden das Krisenmanagement Ebenen übergreifend stärken und die einsatzführenden Stellen vor Ort entlasten.

Außerdem erfolgt eine signifikante Stärkung des BBK sowie der Bundesanstalt Technisches Hilfswerk (THW). Im Vergleich zum Jahr 2019 (die Haushaltsjahre 2020 und 2021 waren durch umfangreiche zusätzliche, jedoch zeitlich befristete Konjunkturmittel geprägt und eignen sich daher nicht als Referenzwert) weist das BBK einen Zuwachs in Höhe von rund 20 Prozent und das THW einen deutlichen Zuwachs von fast 40 Prozent auf. Darüber hinaus hat das BBK im Haushaltsjahr 2022 zusätzlich 112 Planstellen erhalten, von denen bereits 71 besetzt werden konnten. Für das Haushaltsjahr 2023 ist für das BBK ein Aufwuchs um 146 zusätzliche Stellen vorgesehen.

Um die Warnstruktur in ganz Deutschland zu verbessern, stellt die Bundesregierung zudem insgesamt 88 Mio. Euro zum Ausbau kommunaler Sirenennetze zur Verfügung.

Die Bundesregierung arbeitet zusammen mit den Mobilfunknetzbetreibern derzeit mit Hochdruck an der Einführung des neuen Warnkanals Cell Broadcast, mit dessen Hilfe Warnungen als Textnachrichten auf sämtliche Mobiltelefone in einem bestimmten Gebiet versandt werden können, ohne dass der Besitzer zuvor eine App installieren muss. Ende Februar 2023 soll Cell Broadcast den Wirkbetrieb aufnehmen, die bisherigen Warnmittel ergänzen und somit die Warneffektivität in Deutschland nochmals steigern.

Seit dem 1. Juni 2022 läuft das Forschungsvorhaben „ALANO – Eine Analyse alternativer Lagerungsstrategien der öffentlichen Notfallbevorratung von Lebensmitteln“, in dessen Rahmen geprüft wird, inwieweit Anpassungen hinsichtlich der Gestaltung der staatlichen sowie der privaten Vorratshaltung vor dem Hintergrund der Erfahrungen aus der Corona-Krise und dem russischen Angriffskrieg gegen die Ukraine vorgenommen werden können. Vor dem Hintergrund der COVID-19-Pandemie hat die Bundesregierung mit Blick auf eine verbesserte Vorbereitung und Versorgung in mehreren Kabinettbeschlüssen (3. Juni 2020/21. Juli sowie 24. November 2021) entschieden, in drei Phasen eine Nationale Reserve Gesundheitsschutz (NRGS) zu errichten.

Im Wege von Warenbevorratung sowie des Vorhaltens von Produktionskapazitäten und Neuproduktion soll sie den Bedarf des Gesundheitssektors, des Bundes und weiterer Bedarfsträger für bis zu sechs Monate (davon mindestens einen Monat physisch) decken und humanitäre Hilfe durch die Lieferung von Schutzausstattung an die Weltgesundheitsorganisation und Drittstaaten ermöglichen.

Zusätzlich hat das BMI hierzu einen ressortübergreifenden Gemeinsamen Koordinierungsstab Kritische Infrastruktur (GEKKIS) eingerichtet. Auch innerhalb verschiedener Ressorts wurden ähnliche Strukturen zur besseren Koordinierung geschaffen.

16. Welche Maßnahmen trifft die Bundesregierung, um die Thematik in der Nationalen Sicherheitsstrategie zu verankern und eine Umsetzungsstrategie zu ermöglichen?

    Welche Zeiträume sind bis zur Umsetzung vorgesehen?

Die Nationale Sicherheitsstrategie befindet sich derzeit noch in der Abstimmung. Daher können zum jetzigen Zeitpunkt noch keine Aussagen über deren Inhalte oder Umsetzung getroffen werden.

17. Inwiefern sind das Bundesministerium der Verteidigung und die Kommandoinfrastruktur der Bundeswehr einschließlich ihrer Operationszentralen, Lagezentren und Gefechtsstände als kritische Infrastruktur eingestuft, und inwiefern ist die Betriebsbereitschaft auch im Katastrophen- oder Zivilschutzfall sichergestellt?

Die Einrichtungen der Bundeswehr, die als „verteidigungswichtige Infrastruktur“ eingestuft sind, können die Betriebsbereitschaft im Katastrophenfall sicherstellen. Infrastruktur gilt in diesem Kontext dann als verteidigungswichtig, wenn sie unverzichtbar für den Einsatz und die Aufgabenwahrnehmung der Bundeswehr im Rahmen Landes- und Bündnisverteidigung, Dauereinsatzaufgaben sowie dauerhafter zivil-militärischer Kooperationen und Unterstützungsleistungen ist.

18. Wie und mit welchen Kräften erfolgt die Absicherung der kritischen Infrastruktur einschließlich militärischer Liegenschaften, und wer koordiniert diese?

Grundsätzlich sind in Deutschland die Betreiber kritischer Infrastrukturen verantwortlich für deren Schutz. Bei konkreten Gefährdungen von kritischen Infrastrukturen sind die Sicherheitsbehörden in Bund und Ländern zuständig.

Für militärische Liegenschaften gilt: Die Absicherung bzw. Bewachung der Liegenschaft erfolgt im Grundbetrieb grundsätzlich durch zivile Wachunternehmen.

Die Absicherung einer Liegenschaft kann bei Erhöhung der Gefährdungsstufe, z. B. bei konkret vorliegenden Bedrohungslagen, durch Einsatz von militärischen Kräften verstärkt werden.

19. Inwiefern wurden im Cyber- und Informationsraum der Bundeswehr Vorsorgemaßnahmen getroffen, um möglichen Sabotageakten vorzubeugen bzw. reaktionsfähig zu begegnen?

Die Bundeswehr verfügt sowohl über defensive und offensive Cyberverteidigungsfähigkeiten zur Aufklärung und Wirkung im Cyberraum, als auch über defensive Cyberverteidigungsfähigkeiten zur Verhinderung, Erkennung und Bewältigung von Cyberangriffen gegen die IT der Bundeswehr im In- und Ausland. Darüber hinaus arbeitet die Bundeswehr ressortübergreifend eng mit den Behörden der Inneren Sicherheit, insbesondere über das Nationale Cyberabwehrzentrum und mit internationalen Partnern zusammen. Darüber hinaus werden die IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umgesetzt.

20. Ist der Internetknoten DE-CIX inklusive seiner Rechenzentren nach Auffassung der Bundesregierung Teil der kritischen Infrastruktur in Deutschland?

a) Ab welcher Datendurchsatzrate stuft die Bundesregierung Internetknoten als kritische Infrastruktur ein?

Die derzeit unter die BSI-Kritisverordnung fallenden Anlagen im Sektor IKT sind z. B. unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/bsi-kritisverordnung-poster.pdf?__blob=publicationFile&v=3 einsehbar. Zu ihnen gehören auch sogenannte Internet Exchange Points (IXP) für öffentlich zugängliche Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste. Als Bemessungskriterium wird in der BSI-Kritisverordnung nicht die Datendurchsatzrate, sondern die Anzahl der angeschlossenen autonomen Systeme betrachtet. Ab einem Schwellenwert von 100 gilt eine Anlage als kritische Infrastruktur. Der in der Fragestellung genannte Internetknoten erfüllt diese Kriterien und gehört somit zu den kritischen Infrastrukturen.

b) Hat die Bundesregierung die Sicherheitsmaßnahmen nach dem 24. Februar 2022 sowohl auf Cybersicherheitsebene als auch auf physischer Ebene für die Internetknoten und zentralen Telekommunikationskabel in Deutschland verstärkt?

Gemäß § 8a des BSI-Gesetzes sind die Betreiber kritischer Infrastrukturen selbst verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.

c) Verfügt die Bundesregierung über ein aktuelles Gesamtmonitoring aller Internetknotenpunkte und zentralen Telekommunikationskabel im Hoheitsgebiet der Bundesrepublik Deutschland?

Die Bundesregierung verfügt nicht über ein aktuelles Gesamtmonitoring aller Internetknotenpunkte und zentralen Telekommunikationskabel im Hoheitsgebiet der Bundesrepublik Deutschland.

21. Inwiefern ist der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben als kritische Infrastruktur eingestuft, und ist dessen Betriebsbereitschaft auch im Katastrophen- oder Zivilschutzfall, z. B. im Fall eines großflächigen und länger anhaltenden Stromausfalls, sichergestellt (z. B. über ein redundantes Kommunikationssystem)?

Der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Digitalfunk BOS) ist nicht als kritische Infrastruktur i. S. des BSIG eingestuft. Zur Sicherstellung der Betriebsbereitschaft des Digitalfunks im Katastrophen- oder Zivilschutzfall wurde ein umfassendes Notfall- und Krisenmanagementsystem etabliert.

Die Bundesregierung hat sich mit den Ländern im Jahr 2011 auf die Einteilung von neun KRITIS-Sektoren verständigt. Dieser Beschluss stellt keine gesetzliche Regelung dar. Es handelt sich um eine Einteilung, welche dennoch das Verständnis der Bundesregierung hinsichtlich der Frage der Definition von kritischen Infrastrukturen mitprägt. Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) fällt bei dieser Einteilung unter den KRITIS-Sektor „Staat und Verwaltung“.

22. Inwiefern sind die Zivile Notfallreserve für Reis, Hülsenfrüchte und Kondensmilch sowie die Bundesreserve Getreide als kritische Infrastrukturen eingestuft, und inwiefern sind diese Reserven auch im Katastrophen- oder Zivilschutzfall, z. B. im Fall eines großflächigen und länger anhaltenden Stromausfalls, sichergestellt und funktionsfähig?

Die Zivile Notfallreserve sowie die Bundesreserve Getreide sind grundsätzlich der kritischen Infrastruktur „Ernährung“ zuzurechnen. Die Vorräte sind indessen nicht allgemein für Zwecke des Katastrophenschutzes bestimmt, sondern sollen bei der Überbrückung kurzfristiger Engpässe bei der Versorgung der Bevölkerung mit Lebensmitteln helfen. Sollte ein Stromausfall zu einer Versorgungskrise führen, kann – vorbehaltlich der verfügbaren Energie- und Logistikkapazitäten – grundsätzlich auf die Notfallvorräte zurückgegriffen werden.

23. Nach welchen Kriterien und Priorisierungen wird kritische Infrastruktur besonders geschützt, und welche Stelle nimmt diese Priorisierung vor?

Auf die Antwort zu Frage 20b wird verwiesen. Zudem erfolgt nach BSI-Gesetz und der BSI-Kritisverordnung keine Priorisierung, sondern lediglich die Feststellung, ob Einrichtungen, Anlagen oder Teile davon als kritische Infrastrukturen im Sinne des BSI-Gesetzes gelten.

24. Inwiefern wurde bei der kritischen Infrastruktur die Überprüfung von vulnerablen (Schnitt)stellen und Akteuren seit dem 24. Februar 2022 durchgeführt?

Erfolgte dies intensiviert?

Grundsätzlich sind in Deutschland die Betreiber kritischer Infrastrukturen verantwortlich für deren Schutz vor Sabotagehandlungen. Bei konkreten Gefährdungen von kritischen Infrastrukturen sind die Sicherheitsbehörden in Bund und Ländern zuständig.

Zusätzlich wurden die Betreiber kritischer Infrastrukturen durch Versand einer Gefährdungsbewertung des Bundeskriminalamtes (BKA) anlässlich von möglichen Sabotageakten auf Nord Stream Pipelines auf die abstrakte Gefährdungslage hingewiesen und entsprechend sensibilisiert. Generell nehmen die Sicherheitsbehörden regelmäßig Gefährdungsbewertungen vor, die fortlaufend der aktuellen Lage angepasst und den Unternehmen sowohl unmittelbar als auch über Wirtschaftsverbände zur Verfügung gestellt werden.

25. Wann werden der Evaluationsbericht sowie der Fortschrittsbericht zur KRITIS (kritische Infrastrukturen)-Strategie vorgelegt, von denen auf der Homepage des Bundesministeriums des Innern und für Heimat die Rede ist (vgl. https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html), und kann die Bundesregierung angesichts der Dringlichkeit bereits erste Schwerpunkte nennen?

Anlässlich des zehnjährigen Bestehens der KRITIS-Strategie hat das BBK einen Bericht zur Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen veröffentlicht (vgl. https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7). Ein Schwerpunkt der Arbeiten der Bundesregierung ist die Erarbeitung und Umsetzung des im Koalitionsvertrags vereinbarten KRITIS-Dachgesetzes. Mit dem KRITIS-Dachgesetz soll das Gesamt-

system beim Schutz kritischer Infrastrukturen in den Blick genommen und dieses resilienter gemacht werden.

26. Wurden zusätzliche Maßnahmen zur Resilienzstärkung kritischer IT-Infrastruktur seit dem 24. Februar 2022 unternommen (bitte einzeln auflisten, welche Maßnahmen wo mit welchem Ziel verfolgt werden)?

Die Stärkung der Resilienz liegt in der Zuständigkeit der Betreiber kritischer Infrastrukturen.

27. Welche Maßnahmen unternimmt die Bundesregierung für die Responsive-Space-Fähigkeit (Fähigkeit, Zugang zu Informationen und Kommunikationswegen über Satellitensysteme im Falle einer Störung oder eines Angriffs aufrechtzuerhalten) Deutschlands?

Die Bundeswehr berücksichtigt die Responsive-Space-Fähigkeit bei der Planung und Realisierung von Projekten im Bereich Satellitenkommunikation. Aufgrund langfristiger Realisierungszeiten und wirtschaftlicher Aspekte werden insbesondere bi- und multinationale Kooperationen mit Bündnispartnern geprüft und, soweit nutzbringend und möglich, umgesetzt. Hierzu zählen beispielsweise das europäische zivil/militärische Vorhaben „European Space-based Secure Connectivity“ oder Aktivitäten der US Space Force mit vergleichbarer Zielsetzung.

28. Welche Vorsorgemaßnahmen hat die Bundesregierung getroffen bzw. in Planung, um im Fall eines Anschlags, einer Sabotage oder eines Cyberangriffes auf bzw. von Energieinfrastruktur negative Auswirkungen zu minimieren?

Die für die Sicherheit und Zuverlässigkeit des Stromversorgungssystems verantwortlichen Übertragungsnetzbetreiber (ÜNB) tragen Vorsorge, um Störungen im Stromnetz bewältigen zu können. Dazu gehören insbesondere – für den Fall eines Ausfalls der Stromversorgung – die Netz- und Versorgungswiederaufbaupläne der ÜNB, die regelmäßig überprüft und aktualisiert werden.

Auch im Mineralölbereich sind grundsätzlich die Betreiber der kritischen Infrastruktureinrichtungen für die Absicherung gegen mögliche Sabotageakte zuständig. Anschläge auf kritische Bereiche der Ölinfrastruktur (Pipelines, Raffinerien, Tanklager) können trotz der bestehenden baulichen Sicherheitsvorkehrungen (Zugangsbeschränkungen, Überdeckung von Pipelines etc.) nicht gänzlich ausgeschlossen werden, da es unmöglich ist, sämtliche Einrichtungen ständig und flächendeckend zu überwachen.

Im Falle eines Anschlags auf eine der genannten Infrastrukturen und Einrichtungen muss daher auf andere Transport- und Versorgungsoptionen ausgewichen werden (z. B. Transport von Rohöl per Bahn oder Schiff) oder es müssen vermehrt Ölprodukte statt Rohöl importiert werden. Im Notfall können strategische Reserven (Rohöl oder Ölprodukte) aus den Beständen des Erdölbevorratungsverbandes freigegeben werden.

29. Welche Maßnahmen werden für den Fall eines großflächigen und länger andauernden Stromausfalls vonseiten der Bundesregierung ergriffen, um die Funktionsfähigkeit von Einrichtungen der kritischen Infrastruktur, insbesondere auch der Sicherheitsbehörden und Einrichtungen des Gesundheitswesens, aufrechtzuerhalten?

Für den Fall eines Ausfalls der Stromversorgung ist es oberste Priorität der verantwortlichen Stromnetzbetreiber, die Stromversorgung möglichst schnell wieder sicherzustellen. Die von den ÜNB vorgehaltenen Netz- und Versorgungswiederaufbaupläne decken auch den Fall eines flächendeckenden Ausfalls ab.

Im Fall eines Ausfalls der Stromversorgung oder bei einer gezielten Abschaltung durch den Netzbetreiber im Falle einer Gefährdung oder Störung der Sicherheit und Zuverlässigkeit des Elektrizitätsversorgungssystems wäre eine Versorgung nur noch durch Notstromaggregate möglich. Dabei obliegt die Entscheidung, ob eine Weiterversorgung über Notstromaggregate sinnvoll oder erforderlich ist, jedem Einzelnen bzw. insbesondere den Betreibern von kritischer Infrastruktur. Besonders schützenswerte Einrichtungen wie beispielsweise Krankenhäuser sind in der Regel mit Notstromaggregaten ausgestattet, um sich unabhängig von den Netzen der öffentlichen Versorgung für einen begrenzten Zeitraum eigenständig mit Elektrizität versorgen zu können. Es wird in diesem Zusammenhang auf den Leitfaden des BBK zur „Notstromversorgung in Unternehmen und Behörden“ verwiesen, der unter folgendem Link abgerufen werden kann:

https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-13-notstromversorgung-unternehmen-behoerden.pdf?__blob=publicationFile&v=8.

Das BBK empfiehlt, eine Notstromversorgung so auszulegen, dass ohne weitere Kraftstoffzufuhr ein Betrieb über 72 Stunden möglich ist.

30. Inwiefern ist die Kontrolle der deutschen Hoheitsgewässer durch die Bundespolizei und/oder Bundeswehr intensiviert worden, und erfolgt in diesem Zusammenhang eine stärkere Aufklärung und Beobachtung entsprechender Routen der kritischen Infrastruktur?

Das deutsche Staatsgebiet erstreckt sich bis zur Grenze des Küstenmeeres, der sogenannten 12-Meilen-Zone. Die Bundespolizei nimmt auf Nord- und Ostsee ihre Aufgaben nach § 2 des Bundespolizeigesetz (BPolG) (Grenzschutz) wahr. Hierzu zählt auch die grenzpolizeiliche Überwachung des Küstenmeeres.

Darüber hinaus nimmt die Bundespolizei auch Aufgaben nach § 6 BPolG (Aufgaben auf See) sowie andere übertragene Aufgaben außerhalb des deutschen Küstenmeeres wahr. Dabei wird die Ausschließliche Wirtschaftszone auf Nord- und Ostsee regelmäßig überwacht. Die Bundespolizei hat im Rahmen ihrer Zuständigkeiten die Überwachung der kritischen Infrastrukturen, insbesondere im Bereich der Ostsee, mit den verfügbaren Einsatzmitteln (Einsatzschiffe und -boote, Polizeihubschrauber) verstärkt.

Der Seefernaufklärer der Deutschen Marine wird neben den Standard-Einsatzverpflichtungen in Nord- und Ostsee aktuell auch für die Überwachung der kritischen Off-Shore-Infrastruktur (OSI) in Norwegen eingesetzt. Dies geschieht in enger Abstimmung mit der NATO. Die Marine war zudem in der 41. Kalenderwoche 2022 im Rahmen der Amtshilfe zur Unterstützung der Bundespolizei bei der Untersuchung der Schadensbilder Nord Stream 1 und 2 eingesetzt. Darüber hinausgehende Amtshilfeersuchen für eine erhöhte Präsenz in deutschen Hoheitsgewässern liegen derzeit nicht vor.

Im Übrigen wird auf die Antwort zu Frage 11 verwiesen.

31. Inwiefern gibt es seitens der Bundesregierung Pläne und Vereinbarungen mit den Ländern, den Schutz der deutschen Küstengebiete an Nord- und Ostsee zu verstärken?

Der Schutz der deutschen Küstengebiete an Nord- und Ostsee wird durch Bund und Länder in ihrer jeweiligen Zuständigkeit wahrgenommen. Die Sicherheitsbehörden in Bund und Ländern stehen im engen Austausch untereinander. Daher gibt es über die bestehenden Zuständigkeiten und Kooperationen hinaus keine neuen Pläne oder Vereinbarungen im Sinne der Fragestellung.

32. Welche konkreten Maßnahmen hat die Bundesregierung seit Beginn der Legislaturperiode ergriffen, um präventiv gegen mögliche Straftaten von Extremisten und „Aktivisten“ auf hochsensible Bereiche der kritischen Infrastruktur vorzugehen?

Das BKA beobachtet fortlaufend die Gefährdung im Hinblick auf die o. g. Angriffsziele und erstellt im Rahmen seiner Zentralstellenfunktion gemäß § 2 BKAG Gefährdungslagebilder und -analysen. Entsprechende Ergebnisse werden turnusmäßig oder anlassbezogen den zuständigen Behörden zur eigenen Beurteilung auch hinsichtlich örtlich/regional zu treffender Maßnahmen zur Verfügung gestellt.

Darüber hinaus erfolgt ein regelmäßiger Informationsaustausch im Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ).

Im Rahmen des gesetzlichen Auftrags nach § 3 Absatz 1 BVerfSchG beobachtet das BfV die Handlungen von Extremisten aller Phänomenbereiche auch im Hinblick auf mögliche Straftaten zum Nachteil kritischer Infrastrukturen. Die erlangten Erkenntnisse fließen regelmäßig auch in öffentlich zugängliche Lagebilder des Bundesamtes für Verfassungsschutz ein.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

33. Inwiefern stimmt sich die Bundesregierung im Rahmen ihrer Maßnahmenplanung zum Schutz kritischer Infrastrukturen mit anderen Staaten und innerhalb der EU ab?

Das BMI ist in den entsprechenden Arbeitsgruppen innerhalb der EU vertreten und stimmt sich regelmäßig mit den anderen Mitgliedstaaten ab, um ein hohes Sicherheitsniveau beim Cyberschutz und beim physischen Schutz kritischer Infrastrukturen in Europa zu erreichen. Gleichzeitig wird auch aktiv an der Anpassung des entsprechenden EU-Rechtsrahmens mitgearbeitet, z. B. an der Richtlinie über die Sicherheit von Netz- und Informationssystemen 2.0 (NIS2-Richtlinie) und der Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie).

34. Welche Maßnahmen sind nach Kenntnis der Bundesregierung derzeit auf europäischer Ebene in Planung, um sich auf großflächige und länger andauernde Stromausfälle sowie andere Notlagen vorzubereiten?

Die ÜNB sind gesetzlich für die Sicherheit und Zuverlässigkeit des Stromversorgungssystems verantwortlich. Das heißt, dass die ÜNB sicherstellen müssen, dass Großstörungen oder gar Netzzusammenbrüche durch geeignete Maßnahmen verhindert werden können. § 13 des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) gibt den ÜNB die Maßnahmen vor, die für die Aufrechterhaltung eines sicheren Netzbetriebs ergriffen werden können.

Nach der Verordnung (EU) 2017/2196 zur Festlegung eines Netzkodex über den Notzustand und den Netzwiederaufbau des Übertragungsnetzes (NC ER) sind alle ÜNB im europäischen Synchronverbund verpflichtet, einen Systemschutzplan* aufzustellen, der die hierfür notwendigen Maßnahmen beschreibt. Auch für die Netz- und Versorgungswiederaufbaupläne der ÜNB macht die Verordnung (EU) 2017/2196 Vorgaben, um auf europäischer Ebene einheitliche Standards zu etablieren. Im Übrigen wird auf die Antworten zu den Fragen 28 und 29 verwiesen.

35. Mit welcher Kommunikationsstrategie sensibilisiert die Bundesregierung die deutsche Bevölkerung über hybride Bedrohungslagen, wie das gezielte Verbreiten von Desinformationen von ausländischen Akteuren, und wie stärkt sie konkret die Resilienz der Bevölkerung?

Unter der Leitung des BMI tagt die Arbeitsgruppe (AG) Hybrid, die der strategischen Koordination des Umgangs mit hybriden Bedrohungen auf Ebene der Bundesregierung dient. Unter anderem werden in diesem Rahmen öffentliche kommunikative Maßnahmen abgestimmt. Nach Beginn des russischen Angriffskrieges gegen die Ukraine wurde unter Federführung des BMI innerhalb der AG Hybrid auf Arbeitsebene die ressortübergreifende Unterarbeitsgruppe Russland/Ukraine (UAG RUS/UKR) eingerichtet. Im Mittelpunkt stehen Maßnahmen zur Identifizierung russischer Narrative, zur Stärkung der faktenbasierten Kommunikation und zur Erhöhung der gesellschaftlichen Resilienz gegen Bedrohungen aus dem Informationsraum.

Ziel ist insbesondere eine Sensibilisierung der Öffentlichkeit zum Thema Desinformation und eine Förderung der Nachrichten- und Medienkompetenz der Bürgerinnen und Bürger, insbesondere zu sozialen Netzwerken. Verschiedene Projekte zur Stärkung der Nachrichtenkompetenz zielen u. a. auf die Befähigung zur kritischen Überprüfung von Informationen und Quellen. Die Bundesregierung setzt sich zudem u. a. mit einer Soforthilfe für geflüchtete Medienschaffende aus der Ukraine, Russland und Belarus für die Stärkung von Exilmedien ein, die mit kritischer und unabhängiger Berichterstattung über ihre Heimatländer oft eine besonders hohe Glaubwürdigkeit besitzen und aktiv Desinformation entgegentreten.

Die UAG RUS/UKR hat ein sogenanntes FAQ, ein Dokument mit häufig gestellten Fragen, zu Desinformation im Kontext des russischen Angriffskrieges gegen die Ukraine sowie einen sogenannten Onepager, ein Informationsblatt, mit dem Titel „Gemeinsam gegen Desinformation“ erstellt. Die Dokumente dienen der Sensibilisierung der Bevölkerung. Sie wurden online veröffentlicht und breit verteilt unter anderem an die Länder und ihre Kommunen sowie an Multiplikatoren in der Zivilgesellschaft u. a. der russland-deutschen Community. Die Dokumente sind in mehreren Sprachen verfügbar, auch auf Russisch.

Verschiedene Ressorts der Bundesregierung stellen zahlreiche Informationen im Internet zur Verfügung u. a.:

Das Bundespresseamt (BPA) informiert auf der Seite der Bundesregierung zum Umgang mit Desinformation: https://www.bundesregierung.de/breg-de/themen/umgang-mitdesinformation.

Das BPA informiert auf der Seite der Bundesregierung auch zum Ukraine-Krieg: https://www.bundesregierung.de/breg-de/themen/krieg-in-der-ukraine.

* Der Systemschutzplan der vier deutschen ÜNB kann unter folgendem Link herunter geladen werden: https://www.netztransparenz.de/portals/1/Content/EU-Network-Codes/ER-VErordnung/Systemschutzplan%20der%20%C3%9CNB%20-%20Hauptdokument.pdf

Das BMI informiert über die aktuelle Bedrohungslage hinsichtlich Desinformation als Mittel illegitimer Einflussnahme fremder Staaten, also sogenannter hybrider Bedrohungen: https://www.bmi.bund.de/SharedDocs/topthemen/DE/topthema-desinformation/artikel-desinformation-hybride-bedrohung.html.

Umfangreiche Hinweise und Hintergründe zum Umgang mit Desinformation finden Sie auch auf der Seite der Bundeszentrale für politische Bildung (bpb): https://www.bpb.de/themen/medien-journalismus/desinformation.

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