21. Wahlperiode

Drucksache **21/4704**

HESSISCHER LANDTAG

29. 06. 2026

Eilausfertigung

Antwort

der Landesregierung

Große Anfrage

vom 13.01.2026

Pascal Schleich (AfD), Sandra Weegels (AfD), Bernd Vohl (AfD), Christian Rohde (AfD), Volker Richter (AfD), Markus Fuchs (AfD) und Andreas Lichert (AfD)

Aktueller Stand und Maßnahmen zum Schutz kritischer Infrastrukturen (KRITIS) in Hessen

Drucksache 21/3333

Eingegangen am 29. Juni 2026 · **Eilausfertigung** am 29. Juni 2026

26/06/26 Ba

29.06.2026 Hz

INA

Große Anfrage
Pascal Schleich (AfD), Sandra Weegels (AfD), Bernd Vohl (AfD), Christian Rohde (AfD), Volker Richter (AfD), Markus Fuchs (AfD), Andreas Lichert (AfD) vom 13.01.2026
Aktueller Stand und Maßnahmen zum Schutz kritischer Infrastrukturen (KRITIS) in Hessen
Drucksache 21/3333

und

Antwort

Landesregierung

Vorbemerkung Fragesteller:

Nach dem linksextremen Terroranschlag durch die sogenannte „Vulkangruppe“ auf die kritische Infrastruktur der Bundeshauptstadt Berlin und ihren gravierenden Folgen, stellt sich die Frage wie die hessische Landesregierung die kritische Infrastruktur in Hessen aktuell schützt.

Vorbemerkung Landesregierung:

Kritische Infrastrukturen (KRITIS) sind Organisationen, Einrichtungen und Anlagen mit wesentlicher Bedeutung für das staatliche Gemeinwesen. Ihr Ausfall oder ihre Beeinträchtigung kann zu erheblichen Versorgungsengpässen, Störungen der öffentlichen Sicherheit oder anderen schwerwiegenden Folgen führen.

Die Landesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass einzelne Fragen nicht oder nur eingeschränkt beantwortet werden können. Die öffentliche Beantwortung bestimmter Informationen würde Rückschlüsse auf Standorte, Schutzmaßnahmen, Redundanzen, Vorsorgeplanungen, Gefährdungslagen oder bestehende Bewältigungskapazitäten Kritischer Infrastruktur ermöglichen. Dies könnte die Sicherheit betroffener Einrichtungen, der dort eingesetzten Einsatz- und Sicherheitskräfte sowie der Betreiber Kritischer Infrastruktur beeinträchtigen.

Auch in ihrer Gesamtheit oder in Verbindung mit anderen öffentlich zugänglichen Informationen können einzelne Angaben geeignet sein, Rückschlüsse auf sicherheitsrelevante Schwerpunktsetzungen, Schutz- und Sicherheitsstrukturen oder

mögliche Schwachstellen zuzulassen. Die Kenntnis solcher Informationen könnte missbräuchlich verwendet werden und dadurch Nachteile für die Sicherheit Kritischer Infrastruktur sowie die öffentliche Sicherheit insgesamt begründen.

Die Landesregierung sowie der Hessische Landtag haben sich in der laufenden Wahlperiode bereits wiederholt und umfassend mit Fragen der Resilienz, des Schutzes Kritischer Infrastrukturen, der Cybersicherheit sowie der Krisen-, Zivil- und Katastrophenschutzvorsorge befasst; ergänzend wird insoweit auf die Drucksachen 21/727, 21/198, 21/2650, 21/1717, 21/1216, 21/947, 21/946, 21/3195, 21/2837, 21/2825, 21/2784, 21/3646, 21/3455, 21/3361, 21/3314 und 21/3308 sowie auf die hierzu erfolgten Plenar- und Ausschussbefassungen des Hessischen Landtags verwiesen. Die in früheren Drucksachen enthaltenen Ausführungen erfolgten unter den jeweiligen tatsächlichen und sicherheitsrelevanten Rahmenbedingungen. Art und Umfang der Beantwortung bestimmt sich jeweils nach den Umständen des Einzelfalls.

Diese Vorbemerkungen vorangestellt, beantworte ich die Große Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, dem Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigten des Landes beim Bund, dem Minister der Finanzen, dem Minister der Justiz und für den Rechtsstaat, dem Minister für Kultus, Bildung und Chancen, dem Minister für Wissenschaft und Forschung, Kunst und Kultur, dem Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum, der Ministerin für Digitalisierung und Innovation, dem Minister für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat, der Ministerin für Familie, Senioren, Sport, Gesundheit und Pflege sowie der Ministerin für Arbeit, Integration, Jugend und Soziales für die Landesregierung wie folgt:

Frage 1. Wie erfolgt die Klassifizierung markanter Einrichtungen und Objekte der Infrastruktur in Hessen als kritische Infrastruktur?

Frage 2. Welche Stufen der Priorisierung der hessischen Einrichtungen und Objekte kritischer Infrastruktur gibt es?

Frage 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Grundlage für die systematische Erfassung und Klassifizierung Kritischer Infrastrukturen in Hessen bildet die unter www.kritis.hessen.de verfügbare Übersicht der KRITIS-relevanten Sektoren, Branchen und kritischen Dienstleistungen. Diese Systematik gliedert die Kritischen Infrastrukturen in Hessen nach einem dreistufigen Klassifizierungsrahmen: Sektoren bilden die übergeordnete Ebene, darunter sind die jeweiligen Branchen verortet, und auf der operativen Ebene werden die konkreten kritischen Dienstleistungen ausgewiesen.
Eine weitergehende Klassifizierung und faktische Priorisierung von KRITIS-Betreibern erfolgt durch die Regelungen des IT-Sicherheitsgesetzes des Bundes sowie die noch in Rechtsverordnungen zu konkretisierenden Regelungen des KRITIS-Dachgesetzes.

Zentrales Kriterium ist hierbei ein Schwellenwert von 500.000 zu versorgenden Einwohnerinnen und Einwohnern je Anlage, der durch die BSI-Kritisverordnung (BSI-KritisV) in sektorspezifische, technische Leistungswerte überführt und operationalisiert wurde.
Darüber hinaus gibt es keine weitere Unterteilung in Gefährdungs- oder Priorisierungsstufen.

Frage 3. Welche Städte in Hessen weisen die höchste Anzahl an Einrichtungen und Objekten kritischer Infrastruktur auf?

Es wird auf die Vorbemerkung verwiesen.

Frage 4. Wie viele Organisationen oder Gruppierungen des Rechtsextremismus, Linksextremismus, auslandsbezogenen Extremismus sowie religiösen Extremismus werden jeweils vom Landesamt für Verfassungsschutz aufgrund des Verdachts der Vorbereitung terroristischer Aktivitäten beobachtet? Bitte die Anzahl jeweils für die letzten fünf Jahre angeben.

Das Landesamt für Verfassungsschutz Hessen (LfV Hessen) beobachtet im Rahmen seines gesetzlichen Auftrags extremistische Bestrebungen. Terrorismusbezüge können dabei je nach Organisation oder Gruppierung unterschiedlich ausgeprägt sein.

Eine trennscharfe Zuordnung ist daher nicht in allen Fällen möglich.

Für den Betrachtungszeitraum kann folgendes mitgeteilt werden: Im Phänomenbereich Rechtsextremismus einschließlich Reichsbürger und Selbstverwalter wurden mehrere Organisationen beziehungsweise Gruppierungen (2021: vier; 2022: fünf; 2023: fünf; 2024: vier; 2025: sechs), im Phänomenbereich Linksextremismus keine, im Phänomenbereich auslandsbezogener Extremismus drei und im Phänomenbereich Islamismus vier Organisationen bzw. Gruppierungen im Sinne der Fragestellung beobachtet.

Frage 5. Welche politisch motivierten Hintergründe (z. B. Rechtsextremismus, Linksextremismus, auslandsbezogenen Extremismus sowie religiösen Extremismus) wurden bei Angriffen auf staatliches Eigentum in Hessen in den letzten fünf Jahren festgestellt? Bitte nach Jahren aufschlüsseln.

Frage 7. Gegen wie viele Einrichtungen und Objekte kritischer Infrastruktur in Hessen wurden in den letzten fünf Jahren Anschläge oder Anschlagsversuche verübt oder vereitelt?

Frage 8. Wie viele Angriffe oder Anschlagsversuche auf staatliches Eigentum des Bundes oder des Landes Hessen, insbesondere auf Liegenschaften oder sonstige Sachwerte von Behörden oder Sicherheitsorganen, wurden in den letzten fünf Jahren in Hessen registriert?

Die Fragen 5, 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Datengrundlage bildet der Kriminalpolizeiliche Meldedienst in Fällen Politisch motivierter Kriminalität (KPMD-PMK). Ausweislich der polizeilichen Statistik können folgende Fallzahlen genannt werden. Die Auswertung betrifft allgemeine Angriffe auf staatliches Eigentum und basiert nicht auf einer spezifischen KRITIS-Zuordnung.

Jahr	Fallzahlen	Phänomenbereich
2021	244	46x PMK -rechts- 13x PMK -links- 10x PMK -ausländische Ideologie- 175x PMK -nicht zuzuordnen-
2022	127	16x PMK -rechts- 8x PMK -links- 4x PMK -ausländische Ideologie- 99x PMK -nicht zuzuordnen-
2023	248	32x PMK -rechts- 35x PMK -links- 16x PMK -ausländische Ideologie- 2x PMK -religiöse Ideologie- 163x PMK -sonstige Zuordnung-
2024	374	67x PMK -rechts- 56x PMK -links- 18x PMK -ausländische Ideologie- 233x PMK -sonstige Zuordnung-
2025	850	148x PMK -rechts- 425x PMK -links- 25x PMK -ausländische Ideologie- 252x PMK -sonstige Zuordnung-

Anmerkung: Der Phänomenbereich PMK -nicht zuzuordnen- wurde zum 1. Januar 2023 inhaltsgleich in den Phänomenbereich PMK -sonstige Zuordnung- überführt.

Ergänzend wird auf die Kleine Anfrage Drs. 21/3455 verwiesen.

Frage 6. Wurden nach den jüngsten Brandanschlägen auf staatliches Eigentum in Hessen bestehende Sicherheits- und Schutzkonzepte überprüft oder angepasst, wenn ja, in welcher Form?

Die Überprüfung und Anpassung von Sicherheits- und Schutzkonzepten ist laufender

Bestandteil der Arbeit der Sicherheitsbehörden. Vorfälle werden anlassbezogen ausgewertet und bestehende Konzepte bei Bedarf fortgeschrieben oder angepasst. Darüber hinaus findet zwischen den zuständigen Landes- und Bundesbehörden ein fortlaufender Informationsaustausch statt.

Frage 9. Wie viele Angriffe oder Anschlagsversuche richteten sich in den letzten fünf Jahren konkret gegen Liegenschaften oder Einrichtungen der Bundeswehr in Hessen?

Die Datengrundlage bildet der KPMD-PMK. In den Jahren 2021, 2023 und 2024 wurden keine Fälle registriert, im Jahr 2022 drei Fälle und im Jahr 2025 13 Fälle.

Frage 10. Wie viele Angriffe, Anschläge oder Sachbeschädigungen wurden in den letzten fünf Jahren in Hessen gegen staatliche Fahrzeuge, insbesondere Fahrzeuge von Polizei, Bundeswehr, Zoll, Justiz oder kommunalen Behörden, verübt?

Die Datengrundlage bildet der KPMD-PMK. Im Jahr 2021 wurden acht Fälle registriert, im Jahr 2022 sechs Fälle, im Jahr 2023 vier Fälle, im Jahr 2024 zwei Fälle und im Jahr 2025 15 Fälle.

Frage 11. Wie viele Ermittlungsverfahren gegen Tatverdächtige, die einen Anschlag auf Einrichtungen oder Objekte kritischer Infrastruktur geplant oder vollendet haben, gab es in den letzten fünf Jahren in Hessen?

Es wird auf die Kleine Anfrage Drs. 21/3455 verwiesen. In allen in der Beantwortung der Frage 1 aufgezählten Fällen wurde durch die hessische Polizei ein Ermittlungsverfahren eingeleitet.

Frage 12. Wie viele Menschen wurden in Hessen in den letzten fünf Jahren durch

versuchte und/oder vollendete Anschläge auf Einrichtungen oder Objekte kritischer Infrastruktur verletzt oder getötet?

Aufgrund fehlender, mit der konkreten Fragestellung übereinstimmender Erhebungs- und/oder Erfassungsparameter im KPMD-PMK wurden Angriffsziele ausgewertet, die typischerweise einen möglichen Bezug zur Kritischen Infrastruktur aufweisen. Es wurden keine Tötungsdelikte im Abfragezeitraum registriert. Im Zusammenhang mit Körperverletzungsdelikten wurde im Jahr 2021 ein Fall, im Jahr 2022 vier Fälle und im Jahr 2023 ein Fall und in den Jahren 2024 und 2025 kein Fall registriert.

Frage 13. Wie hoch ist der monetäre Schaden, der durch versuchte und/oder vollendete terroristische Anschläge auf Einrichtungen oder Objekte kritischer Infrastruktur in den letzten fünf Jahren in Hessen entstanden ist?

Frage 14. In welcher Höhe wurde der entstandene Schaden durch ermittelte und verurteilte Täter ersetzt?

Die Fragen 13 und 14 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Landesregierung liegen keine validen Daten im Sinne der Fragestellung vor.

Frage 15. Ist die hessische Landesregierung über Anschläge gegen Einrichtungen oder Objekte der Deutschen Bahn, die sich in Hessen befinden, durch die für die Deutsche Bahn zuständigen Bundesbehörden informiert worden?

Zwischen den Sicherheitsbehörden besteht ein standardisierter sowie anlassbezogener Informationsaustausch und eine enge Zusammenarbeit. Der Landesregierung liegen keine derartigen Meldungen in Bezug auf Einrichtungen oder Objekte der Deutschen Bahn in Hessen vor.

Frage 16. Welche Präventionsmaßnahmen gegen geplante Anschläge auf

Einrichtungen und Objekte kritischer Infrastruktur bestehen aktuell in Hessen?

Die Betreiber Kritischer Infrastruktur sind nach den gesetzlichen Vorgaben grundsätzlich selbst für den Schutz und die Sicherheit ihrer Einrichtungen und Anlagen verantwortlich. Grundlage hierfür sind besonders die Vorgaben des IT-Sicherheitsrechts des Bundes, der BSI-KRITIS-Verordnung sowie des KRITIS-Dachgesetzes.

Die Sicherheitsbehörden stehen mit den Betreibern Kritischer Infrastruktur in einem engen und kooperativen Austausch (Informationsaustausch, Sensibilisierung, Lagebewertung, gemeinsame Austausch- und Kooperationsformate wie den Runden Tisch KRITIS).

Das Landesamt für Verfassungsschutz Hessen sowie das Hessische Landeskriminalamt nehmen Aufgaben zur Erkennung, Bewertung und Abwehr von Gefährdungslagen wahr.

Eine weitergehende Beantwortung könnte Rückschlüsse auf sicherheitsrelevante Schwerpunktsetzungen, Gefährdungseinschätzungen und Vorsorgeplanungen zulassen. Soweit operative Präventionsmaßnahmen, Schutzkonzepte oder konkrete Sicherheitsvorkehrungen betroffen sind, verweist die Landesregierung auf die Vorbemerkung.

Frage 17. Welche technischen Einrichtungen, Ausrüstungen (z. B. Notstromaggregate), Notfallpläne, Notunterkünfte, Bevorratungen sowie speziell eingewiesene Rettungskräfte stehen in Hessen für den Fall eines terroristischen Anschlags auf Einrichtungen oder Objekte kritischer Infrastruktur zur Verfügung?

Im Land bestehen Planungen und Vorsorgemaßnahmen für den Fall eines Ausfalls Kritischer Infrastruktur. Hierzu zählen landesweite Rahmenempfehlungen und Sonderschutzpläne sowie ergänzende Vorsorge- und Notfallplanungen der

zuständigen Behörden und Betreiber.

Für die Einrichtung von Notunterkünften und Betreuungsstellen stehen im Katastrophenschutz Betreuungszüge und Einsatzkräfte zur Verfügung. Darüber hinaus wurden unter anderem mobile Notstromaggregate, Netzersatzanlagen sowie Ausstattungen zur Sicherstellung der Kommunikationsfähigkeit beschafft.

Zur Sicherstellung der Einsatz- und Handlungsfähigkeit von Polizeiliegenschaften bestehen gesonderte Vorsorgeplanungen.

Frage 18. Werden bei Übungen von Katastrophenschutz, Rettungsdiensten und Feuerwehr neben angenommenen Unfällen und Naturkatastrophen auch Szenarien terroristischer Anschläge und deren Folgen berücksichtigt?

Ja.

Frage 19. In welchen Landkreisen wurden in den letzten fünf Jahren kreisinterne und kreisübergreifende Übungen zu Szenarien wie MANV, Stromausfall, Naturkatastrophen, Terroranschlägen oder weiteren vergleichbaren Lagen durchgeführt?

In den vergangenen fünf Jahren wurden landesweit zahlreiche Katastrophenschutzübungen und Stabsübungen zu unterschiedlichen Szenarien wie MANV-Lagen, Stromausfällen, Naturkatastrophen und weiteren Großschadenslagen durchgeführt. Darüber hinaus werden die Katastrophenschutz- und Verwaltungsstäbe der unteren Katastrophenschutzbehörden, der Regierungspräsidien sowie der Landesverwaltung regelmäßig geschult und beübt.

Eine weitergehende Darstellung nach einzelnen Landkreisen und konkreten Übungsszenarien könnte Rückschlüsse auf sicherheitsrelevante Schwerpunktsetzungen, Gefährdungseinschätzungen und Vorsorgeplanungen zulassen.

Frage 20. In welchem Umfang werden kritische Infrastrukturen in Hessen gegen Cyberangriffe und hybride Bedrohungen geschützt?

Frage 23. Gibt es verpflichtende IT-Sicherheitsaudits oder verbindliche Mindeststandards für Betreiber kritischer Infrastruktur in Hessen?

Frage 32. Welche gesetzlichen Grundlagen auf Landes- und Bundesebene regeln den Schutz kritischer Infrastruktur in Hessen, und sieht die Landesregierung insoweit Änderungsbedarf?

Die Fragen 20, 23 und 32 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Wie bereits dargelegt, liegt die Verantwortung für den Betrieb Kritischer Infrastruktur grundsätzlich bei den jeweiligen Betreibern. Der Schutz gegen Cyberangriffe und hybride Bedrohungen richtet sich nach den einschlägigen bundes- und landesrechtlichen Vorgaben, insbesondere dem BSI-Gesetz, der BSI-KRITIS-Verordnung, dem Hessischen IT-Sicherheitsgesetz, dem KRITIS-Dachgesetz und den jeweiligen KRITIS-Bereich betreffenden einschlägigen Gesetzen sowie untergesetzlichen Regelungen. Darüber hinaus regeln eine Vielzahl von Normen und verbandlichen Regelungen detailliert die Anforderungen an den Schutz Kritischer Infrastruktur.

Hierzu zählen verbindliche Anforderungen an die Informations- und Cybersicherheit, Meldepflichten bei Sicherheitsvorfällen sowie regelmäßige Nachweise und Audits zur Einhaltung gesetzlicher Mindeststandards. Die gesetzlichen Anforderungen bilden dabei Mindeststandards; weitergehende Schutzmaßnahmen der Betreiber bleiben hiervon unberührt. Mit der Umsetzung der NIS2-Richtlinie wird der bestehende Rechtsrahmen weiterentwickelt.

Darüber hinaus stehen den Betreibern mit dem Hessen CyberCompetenceCenter (Hessen3C) sowie der Zentralen Ansprechstelle Cybercrime für die Wirtschaft (ZAC) beim Hessischen Landeskriminalamt Unterstützungs- und Beratungsangebote zur Verfügung.

Zudem wurde in Zusammenarbeit zwischen dem Landeskommando Hessen, dem Hessischen Industrie- und Handelskammertag (HIHK), der Vereinigung hessischer Unternehmerverbände (VhU) und der Firma GAL Digital GmbH eine App entwickelt, mit der deutsche Unternehmen kostenlos ihre Resilienz prüfen können. Dies unterstützt Betriebe dabei, ihre Widerstandsfähigkeit in Ausnahmesituationen zu prüfen und zu stärken. Das Online-Tool ist kostenlos, die Angaben erfolgen anonym.

Die Landesregierung überprüft den bestehenden Rechtsrahmen fortlaufend unter Berücksichtigung der aktuellen Bedrohungslage sowie bundes- und europarechtlicher Entwicklungen. Ergänzend wird auf die Beantwortung der Frage 2 der Kleinen Anfrage Drucks. 21/622 verwiesen.

Frage 21. Wie viele Cyberangriffe oder IT-Sicherheitsvorfälle gegen Betreiber kritischer Infrastruktur in Hessen wurden in den letzten fünf Jahren registriert?

Der Landesregierung wurden in den letzten fünf Jahren elf Cyberangriffe beziehungsweise IT-Sicherheitsvorfälle mit möglichem Bezug zu Betreibern Kritischer Infrastruktur bekannt. Eine allgemeine Meldepflicht gegenüber der Landesregierung besteht nicht.

Frage 22. Welche Rolle spielt das Hessische CyberCompetenceCenter (Hessen3C) beim Schutz kritischer Infrastruktur?

Hessen3C ist die zentrale Kompetenzstelle zum Thema Cybersicherheit und zur interdisziplinären Zusammenarbeit und institutionalisierten Kooperation staatlicher Behörden. Bei schweren Sicherheitsvorfällen können die Spezialisten des Hessen3C bei der Analyse unterstützen. In Zusammenarbeit mit der Koordinierungsstelle KRITIS in Hessen führt das Hessen3C Sensibilisierungs- und Awarenessveranstaltungen durch. Zudem ist das Hessen3C die zentrale Kontaktstelle des Landes für das BSI (§ 40 Absatz 3 Nr. 4 d Gesetz über das Bundesamt für Sicherheit in der

Informationstechnik (BSIG)).

Frage 24. Wie bewertet die Landesregierung die Resilienz kritischer Infrastrukturen in Hessen im Falle eines längerfristigen Ausfalls, beispielsweise eines mehrtägigen Strom- oder Kommunikationsausfalls?

Die Resilienz Kritischer Infrastrukturen setzt eine fortlaufende Vorsorge, Vorbereitung, Reaktion und Nachsorge voraus. Die Landesregierung hat hierzu in den vergangenen Jahren ressortübergreifende Koordinierungs- und Vorsorgestrukturen entwickelt. Hierzu zählen die Resilienzstrategie des Landes, der Sicherheits- und Resilienzrat sowie der Resilienzplan Hessen.

Für die Aufrechterhaltung der staatlichen Handlungs- und Kommunikationsfähigkeit bei längerfristigen Ausfällen bestehen landesweite Vorsorge- und Rahmenplanungen, die durch kommunale Planungen ergänzt werden. Ergänzend unterstützt das Land Kommunen unter anderem im Rahmen der Initiative „KOMPASS Resilienz“ bei der Stärkung örtlicher Vorsorge- und Krisenstrukturen. Ziel ist es, die kommunale Handlungsfähigkeit in Krisenlagen weiter zu stärken und die Vorbereitung auf großflächige Schadens- und Ausfalllagen vor Ort zu unterstützen.

Soweit sich aus Übungen, Ereignissen oder Lagebewertungen weiterer Handlungsbedarf ergibt, werden bestehende Vorsorge- und Schutzmaßnahmen entsprechend angepasst.

Mit der Erweiterung des Programms KOMPASS um den Baustein Cybersicherheit stärkt die Landesregierung die digitale Widerstandsfähigkeit der hessischen Kommunen. Ergänzend zum Aktionsprogramm Kommunale Cybersicherheit unterstützt sie Städte und Gemeinden dabei, ihre IT-Systeme besser gegen Cyberangriffe und technische Ausfälle zu schützen. Ziel ist es, die Handlungsfähigkeit der Verwaltungen zu sichern und das Vertrauen der Bürger in eine verlässliche digitale Infrastruktur zu stärken.

Im Übrigen wird auf die Beantwortung der Kleinen Anfragen Drucks. 21/3281 und

21/947 verwiesen.

Frage 25. Welche Redundanzen, etwa Ersatzsysteme oder Ausweichstandorte, bestehen bei besonders sensiblen Einrichtungen kritischer Infrastruktur?

Es wird auf die Vorbemerkung verwiesen.

Frage 26. Wie lange würde es nach Einschätzung der Landesregierung dauern, zentrale Einrichtungen kritischer Infrastruktur nach einem schweren Anschlag wieder vollständig in Betrieb zu nehmen?

Die Dauer einer Wiederinbetriebnahme Kritischer Infrastruktur nach einem schweren Anschlag hängt wesentlich von Art und Umfang der Schäden, dem betroffenen Infrastrukturbereich sowie den verfügbaren Wiederherstellungs- und Ersatzkapazitäten ab. Eine pauschale zeitliche Einschätzung ist nicht möglich.

Frage 27. Werden Betreiber kritischer Infrastruktur verpflichtet oder angehalten, eigenes Sicherheitspersonal speziell für Terror- und Krisenszenarien zu schulen?

Bereits vor Inkrafttreten des KRITIS-Dachgesetzes waren die Betreiber Kritischer Infrastruktur im Rahmen ihrer Eigenverantwortung gehalten, angemessene Vorsorge- und Schutzmaßnahmen zu treffen.

Durch das KRITIS-Dachgesetz wurden die Anforderungen an die Risikoanalyse, Resilienzplanung und Schutzmaßnahmen Kritischer Infrastruktur erweitert. Hierzu können auch personelle und organisatorische Maßnahmen gehören.

Frage 28. In welchem Umfang werden Polizei, Feuerwehr und Rettungsdienste in Hessen speziell auf Anschläge gegen Einrichtungen oder Objekte

kritischer Infrastruktur vorbereitet?

Frage 29. Gibt es Personal- oder Ausstattungsdefizite bei Sicherheits- und Rettungsbehörden im Zusammenhang mit dem Schutz kritischer Infrastruktur in Hessen?

Die Fragen 28 und 29 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Sicherheits- und Rettungsbehörden in Hessen berücksichtigen Gefährdungslagen mit möglichem Bezug zu Kritischer Infrastruktur in ihren Einsatz-, Vorsorge- und Ausbildungsplanungen. Die Vorbereitung wird ressort- und ebenenübergreifend sichergestellt.

Das Land Hessen hat in den vergangenen Jahren die Ausstattung des Brand- und Katastrophenschutzes sowie die Vorsorge- und Krisenstrukturen weiter ausgebaut. So wurde die Zahl der im Katastrophenschutz verfügbaren Fahrzeuge in den Landkreisen und kreisfreien Städten auf über 900 Fahrzeuge erhöht. Darüber hinaus stehen rund 80.000 ehrenamtliche Hilfskräfte im Brand- und Katastrophenschutz sowie rund 2.500 hauptamtliche Feuerwehreinsatzkräfte zur Verfügung.

Im Rahmen des Projekts Zivil-Militärische Zusammenarbeit / Zivile Verteidigung (ZMZ/ZV) beim Polizeipräsidium Einsatz werden Aus- und Fortbildungsmaßnahmen zu möglichen Krisen- und Anschlagsszenarien durchgeführt. Das Hessische Landeskriminalamt berücksichtigt Gefährdungslagen mit möglichem Bezug zu Kritischer Infrastruktur in seinen Lagebewertungen und Sensibilisierungsmaßnahmen. An der Hessischen Landesfeuerwehrschule werden unter anderem Führungskräfte, Leitstellenpersonal sowie Krisen- und Verwaltungsstäbe auf Großschadens- und Katastrophenlagen vorbereitet. Übungen zu lebensbedrohlichen Einsatzlagen werden unter Beteiligung von Polizei, Feuerwehr und Rettungsdiensten durchgeführt.
Die Konzepte, Ausstattungen und Vorsorgemaßnahmen werden unter Berücksichtigung neuer Erkenntnisse, Übungen und Bedrohungslagen überprüft und weiterentwickelt. Soweit sich weiterer Anpassungs- oder Ausstattungsbedarf zeigt, wird die Landesregierung auf eine bedarfsgerechte Weiterentwicklung der Sicherheits- und Vorsorgestrukturen hinwirken.

Frage 30. Welche Zuständigkeiten haben Land, Kommunen und Betreiber kritischer Infrastruktur jeweils im Bereich Prävention, Schutz und Wiederherstellung?

Prävention, Schutz und Wiederherstellung Kritischer Infrastruktur obliegen im Grundsatz den jeweiligen Betreibern. Im Übrigen wird auf die vorstehenden Ausführungen zur Verantwortlichkeit der Betreiber Kritischer Infrastruktur verwiesen.

Das Land Hessen nimmt im Bereich des Schutzes Kritischer Infrastruktur koordinierende, vorsorgende und unterstützende Aufgaben wahr. Die jeweils zuständigen Fachressorts und Fachbehörden wirken im Rahmen ihrer Zuständigkeiten an der Vorsorge, Koordinierung und Weiterentwicklung von Schutzmaßnahmen für Kritische Infrastruktur mit.

Die Landkreise und kreisfreien Städte sind als untere Katastrophenschutzbehörden primär für das operative Krisenmanagement und die Gefahrenabwehr vor Ort zuständig. Die Regierungspräsidien nehmen als obere Katastrophenschutzbehörden koordinierende Aufgaben wahr.

Bei landesweiten oder länderübergreifenden Schadenslagen kann das Ministerium des Innern, für Sicherheit und Heimatschutz die einheitliche Lenkung übernehmen und den Krisenstab der Landesregierung einberufen.

Frage 31. Wie ist die Zusammenarbeit zwischen hessischen Sicherheitsbehörden und Bundesbehörden (z. B. BKA, BBK, BSI, Bundespolizei) beim Schutz kritischer Infrastruktur organisiert?

Die Zusammenarbeit zwischen den hessischen Sicherheitsbehörden und den zuständigen Bundesbehörden beim Schutz Kritischer Infrastruktur wird lage-, anlass- und zuständigkeitsbezogen im Rahmen bestehender Koordinierungs- und Austauschstrukturen sichergestellt.

Im polizeilichen Bereich findet ein behördenübergreifender Austausch mit den zuständigen Sicherheitsbehörden des Bundes sowie weiterer Länder regelmäßig sowie objekt- und anlassbezogen statt.

Im Bereich des Schutzes Kritischer Infrastruktur ist die Zusammenarbeit zudem über gemeinsame Bund-Länder-Strukturen und Koordinierungsgremien gesichert. Eine zentrale Rolle nimmt hierbei die Arbeitsgruppe der Koordinierungsstellen Kritische Infrastruktur ein, in der die KRITIS-Koordinierungsstellen der Innenministerien der Länder gemeinsam mit dem Bundesministerium des Innern sowie dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zusammenwirken. Dies dient dem strukturierten Informations- und Erfahrungsaustausch sowie der Abstimmung gemeinsamer Schutz- und Vorsorgemaßnahmen. Die enge Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe umfasst auch methodische Grundlagen, Planungshilfen und Lagebilder für den Bereich der Krisenvorsorge.

Mit dem KRITIS-Dachgesetz wurden die Koordinierungs- und Registrierungsaufgaben des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe weiter ausgebaut.

Im Bereich der Cybersicherheit arbeitet Hessen eng mit dem Bundesamt für Sicherheit in der Informationstechnik sowie den zuständigen Sicherheitsbehörden des Bundes zusammen. Hessen3C vertritt das Land Hessen im Nationalen Cyberabwehrzentrum. Darüber hinaus bestehen gemeinsame Austausch-, Unterstützungs- und Übungsstrukturen im Bereich des IT-Krisenmanagements sowie der Cyberabwehr.

Hessen vertritt gemeinsam mit Niedersachsen die Interessen der Länder im Nationalen Cyber-Sicherheitsrat, in dem Vertreter von Bund, Ländern, Kommunen, Wirtschaft und Wissenschaft zusammenwirken.

Frage 33. Gibt es ressortübergreifende Koordinierungsstellen oder Lagezentren speziell für den Schutz kritischer Infrastruktur in Hessen?

Der Schutz Kritischer Infrastruktur wird grundsätzlich im Rahmen der jeweiligen

fachlichen Zuständigkeiten der Ressorts und Fachbehörden sichergestellt. Soweit Fragestellungen mehrere Zuständigkeitsbereiche betreffen, wird eine ressortübergreifende Abstimmung zwischen den betroffenen Stellen eingeleitet.

Die fachlich zuständigen Ressorts verfügen jeweils über KRITIS-Ansprechpartner für ihren Zuständigkeitsbereich. Für ressortübergreifende Fragestellungen besteht im Ministerium des Innern, für Sicherheit und Heimatschutz zudem die Koordinierungsstelle Kritische Infrastruktur (KoSt KRITIS), die den Informationsaustausch und die Abstimmung zwischen den beteiligten Stellen unterstützt.

Frage 34. Welche Haushaltsmittel stellt das Land Hessen jährlich für den Schutz kritischer Infrastruktur bereit? Bitte nach Jahren aufschlüsseln.

Frage 35. Gibt es Förderprogramme des Landes zur baulichen, technischen oder digitalen Absicherung von Betreibern kritischer Infrastruktur?

Frage 36. Haben Kommunen oder Betreiber kritischer Infrastruktur in den letzten fünf Jahren Fördermittel beantragt oder erhalten, und wenn ja, in welcher Höhe?

Die Fragen 34 bis 36 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Maßnahmen zum Schutz und zur Resilienz Kritischer Infrastruktur werden ressortübergreifend im Rahmen unterschiedlicher Zuständigkeiten und Förderbereiche unterstützt. Dies betrifft unter anderem Maßnahmen der kommunalen Infrastruktur, des Brand- und Katastrophenschutzes, der Digitalisierung, der Notstromvorsorge sowie der Energieversorgungs- und Kommunikationssicherheit.

Eine nach Jahren aufgeschlüsselte Gesamtdarstellung der Haushaltsmittel oder Fördermittel ausschließlich für den Schutz Kritischer Infrastruktur ist nicht möglich. Entsprechende Maßnahmen werden aus unterschiedlichen Haushaltsansätzen und Förderprogrammen verschiedener Ressorts finanziert und nicht gesondert als eigenständige KRITIS-Ausgaben erfasst.

Eine ressortübergreifend zusammengeführte Aufstellung zu Förderanträgen oder bewilligten Fördermitteln ausschließlich mit Bezug zu Kritischer Infrastruktur liegt nicht vor.

Frage 37. Wie werden Bevölkerung und Kommunen über Risiken, Vorsorgemaßnahmen und Verhaltensregeln bei Anschlägen auf kritische Infrastruktur informiert?

Frage 38. Gibt es Warn- und Informationskonzepte speziell für den Ausfall kritischer Infrastruktur, etwa bei Strom-, Wasser- oder Telekommunikationsausfällen?

Die Fragen 37 und 38 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Bei großflächigen Schadenslagen — zu denen je nach Art und Umfang auch Anschläge auf Kritische Infrastruktur zählen — können Rettungskräfte nicht überall gleichzeitig präsent sein. Der Befähigung der Bevölkerung zur Selbsthilfe kommt daher eine elementare Bedeutung zu. Ziel der Landesregierung ist es, die Bürgerinnen und Bürger in die Lage zu versetzen, sich selbst und anderen in einer Notlage helfen zu können, bis staatliche Hilfe eintrifft. Eine handlungssichere Bevölkerung ist dabei kein Selbstzweck, sondern eine wesentliche Voraussetzung für die Gesamtresilienz des Landes.

Zu diesem Zweck hat das Land Hessen in Kooperation mit dem BBK das hessische Konzept zur Vermittlung von Inhalten der Brandschutzerziehung im Schulunterricht gezielt weiterentwickelt. Das Konzept wurde so ausgebaut, dass neben der Brandschutzerziehung nunmehr auch zentrale Themenbereiche des Bevölkerungsschutzes — einschließlich des Verhaltens bei Versorgungsausfällen und anderen Krisenlagen — in den Schulunterricht integriert werden, zielgerichtet und altersgruppenspezifisch aufbereitet.

Ergänzend zur schulischen Vermittlung steht Bürgerinnen und Bürgern umfangreiches

Informationsmaterial zur Verfügung. Zentral ist dabei die Broschüre „Vorsorgen für Krisen und Katastrophen" des BBK, die auch Auswirkungen und Vorsorgemaßnahmen bei Ausfällen der Strom- und Wasserversorgung sowie der Telekommunikation konkret skizziert. Die Verbreitung erfolgt über ein möglichst vielfältiges Spektrum an Kanälen — darunter Veranstaltungen wie der Hessentag oder der Bevölkerungsschutztag — mit besonderem Fokus auf den unteren Katastrophenschutzbehörden und den Feuerwehren als bürgernahe Multiplikatoren.

Für die strukturierte Warnung der Bevölkerung hat das Land Hessen die „Arbeitshilfe Warnen" herausgegeben, die die Abläufe zur Durchführung von Warnmeldungen erläutert und den warnenden kommunalen Stellen konkrete Hinweise für die praktische Umsetzung gibt. Die Arbeitshilfe bildet den landesweiten Rahmen, der durch kommunale Planungen — insbesondere hinsichtlich der Einrichtung von Anlaufstellen und der Sicherstellung der Kommunikation bei Ausfall von Telekommunikationseinrichtungen — ergänzt und konkretisiert wird.

Frage 39. Plant die Landesregierung, regelmäßige öffentliche Lageberichte zum Schutz kritischer Infrastruktur vorzulegen?

Über relevante Entwicklungen und Gefährdungslagen wird lage- und anlassbezogen informiert.

Frage 40. Welche Lehren hat die Landesregierung aus realen Anschlägen, Anschlagsversuchen oder Übungen der letzten fünf Jahre gezogen?

Frage 41. Wurden bestehende Schutzkonzepte nach konkreten Vorfällen angepasst oder fortgeschrieben?

Die Fragen 40 und 41 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Erkenntnisse aus Reallagen, Anschlagsversuchen und Übungen werden ausgewertet und bei der Weiterentwicklung von Krisenplänen, Kommunikationsstrukturen und

Vorsorgemaßnahmen berücksichtigt.

Großübungen wie LÜKEX sowie landesweite Krisenstabsübungen haben die Bedeutung belastbarer Kommunikationswege, klarer Zuständigkeiten sowie die Berücksichtigung von Abhängigkeiten und Kaskadeneffekten zwischen verschiedenen Bereichen Kritischer Infrastruktur verdeutlicht.

Ergänzend wird auf die Antwort zu Frage 6 verwiesen.

Frage 42. Welche zukünftigen Bedrohungsszenarien bewertet die Landesregierung derzeit als besonders relevant für Hessen?

Die Landesregierung verfolgt im Bereich des Bevölkerungsschutzes und der Resilienzplanung einen Allgefahrenansatz. Ziel ist es, ein breites Spektrum möglicher Gefahren und Krisenszenarien sowie deren Wechselwirkungen und Kaskadeneffekte in den Blick zu nehmen.

Derzeit stehen Extremwetterereignisse, Cyberangriffe, hybride Bedrohungen, biologische Gefahren sowie terroristische und extremistische Bedrohungen im besonderen Fokus.

Wiesbaden, 24. Juni 2026

Prof. Dr. Roman Poseck
Staatsminister