Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT
mit Antwort der Landesregierung

Anfrage der Abgeordneten Heike Koehler, André Bock, Jan Bauer, Jonas Pohlmann, Claus Seebeck, Verena Kämmerling, Alexander Wille (CDU)

Antwort des Niedersächsischen Ministeriums für Inneres, Sport und Digitalisierung namens der Landesregierung

Resilienz der Stromversorgung und Schutz kritischer Energieinfrastruktur in Niedersachsen

Anfrage der Abgeordneten Heike Koehler, André Bock, Jan Bauer, Jonas Pohlmann, Claus Seebeck, Verena Kämmerling, Alexander Wille (CDU), eingegangen am 10.02.2026 - Drs. 19/9801,
an die Staatskanzlei übersandt am 12.02.2026

Antwort des Niedersächsischen Ministeriums für Inneres, Sport und Digitalisierung namens der Landesregierung vom 16.03.2026

Vorbemerkung der Abgeordneten

Der jüngste Anschlag auf die Strominfrastruktur in Berlin hat gezeigt, dass kritische Energieinfrastrukturen auch in Deutschland gezielten Angriffen, Sabotagehandlungen und anderen sicherheitsrelevanten Bedrohungen ausgesetzt sind.[1] Die Stromversorgung bildet eine Grundlage für nahezu alle gesellschaftlichen, wirtschaftlichen und staatlichen Funktionen. Störungen oder Ausfälle können erhebliche Auswirkungen auf die öffentliche Sicherheit, die wirtschaftliche Leistungsfähigkeit sowie das Vertrauen der Bevölkerung in staatliche Handlungsfähigkeit haben.[2]

1. Wie bewertet die Landesregierung die aktuelle Bedrohungslage für die Stromversorgung in Niedersachsen?

Kritische Infrastrukturen (KRITIS) wie die Stromversorgung stellen grundsätzlich geeignete Angriffsziele für alle Erscheinungsformen und Ausprägungen der Phänomenbereiche der Politisch motivierten Kriminalität (PMK) dar. Angriffe auf die Sektoren der Strom- und Energieversorgung können sowohl in physischer Form erfolgen als auch durch Cyberangriffe.

Vor dem Hintergrund des andauernden Angriffskrieges Russlands gegen die Ukraine stehen KRITIS stärker als zuvor im Fokus der Sicherheitsbehörden. Fremdstaatliche Akteure versuchen vermehrt, mittels sogenannter hybrider Aktivitäten durch verdeckte Maßnahmen Stabilität anderer Staaten zu nehmen. Ziel solcher Aktivitäten ist es, nationale Interessen zu schwächen, unter anderem durch die Erosion demokratischer Institutionen, die Beeinträchtigung sozialer Strukturen oder die Schädigung wirtschaftlicher, technologischer und militärischer Bereiche. Dies geschieht insbesondere durch (Cyber-)Sabotage und (Cyber-)Spionage.

Vor diesem Hintergrund befindet sich die Bedrohungslage anhaltend auf einem abstrakt hohen Niveau, auch wenn es aktuell keine Hinweise auf konkrete Bedrohungslagen in Niedersachsen gibt.

---

1 https://www.deutschlandfunk.de/wegner-nennt-anschlag-auf-stromversorgung-in-berlin-terrorismus-100.html

2 https://www.tagesspiegel.de/politik/wir-haben-erkennbar-ein-problem-mit-sabotage-was-sich-beim-schutz-kritischer-infrastruktur-andern-muss-15102111.html

2. Welche Gefährdungsszenarien (z. B. Sabotage, Terrorismus, Cyberangriffe, Naturereignisse, technische Großstörungen) werden in landesseitigen Risikoanalysen gegebenenfalls berücksichtigt?

Zentrale Aufgabe der Landesregierung ist es, auch im Falle herausragender Bedrohungen und Schadensfälle die Aufrechterhaltung der Aufgabenwahrnehmung in den Ressortbereichen sicherzustellen.

Innerhalb des Landes Niedersachsen werden spezifische Lösungsstrategien für potenzielle Bedrohungen wie Naturkatastrophen, Cyberangriffe, Sabotageakte und physische Angriffe entwickelt und geplant. Dies ist Teil eines umfassenden Ansatzes zur Stärkung der Resilienz des Landes. Ressortübergreifende Zusammenarbeit innerhalb des Bundeslandes sowie die enge Kooperation mit externen Akteuren sind somit zentrale Säulen zur Stärkung der Resilienz gegenüber vielfältigen Bedrohungen.

Zu beachtende „Elementare Gefährdungen“ sind im BSI-Standard 200-3 aufgeführt und im Risikokatalog dezidiert dargestellt. In Beratungen durch den Fachbereich Wirtschaftsschutz beim Niedersächsischen Verfassungsschutz werden diese regelmäßig thematisiert.

Im Katastrophenschutz obliegt es nach § 7 Abs. 1 Niedersächsisches Katastrophenschutzgesetz den unteren Katastrophenschutzbehörden zu untersuchen, welche Katastrophengefahren in ihrem Bezirk drohen. Durch die Bewertung und Umsetzung auf Ebene der unteren Katastrophenschutzbehörden ist sichergestellt, dass die Heterogenität von Siedlungsstruktur und Versorgungsinfrastruktur bestmögliche Berücksichtigung findet.

3. Welche Erkenntnisse liegen der Landesregierung gegebenenfalls zu besonderen Verwundbarkeiten oder Schwachstellen innerhalb der niedersächsischen Strominfrastruktur vor?

Es kann grundsätzlich nicht ausgeschlossen werden, dass es durch vorsätzliche Angriffe auf die Strominfrastruktur auch in Niedersachsen zu Störungen in der netzgebundenen Stromversorgung kommen kann. Ein neuralgischer Punkt der Stromversorgung ist generell das oberirdische Leitungsnetz mit großer Ausdehnung von bundesweit vielen tausend Kilometer Länge, das oft durch abgelegene oder schwer zugängliche Gebiete verläuft, was eine lückenlose Überwachung und somit den physischen Schutz erschwert. Die unmittelbare Einbindung der Stromversorgung in Niedersachsen über die Stromnetze in das bundesweite Stromsystem verdeutlicht zugleich, dass energieseitige Gefährdungsszenarien grundsätzlich bundesweit zu betrachten sind.

Die Bundesregierung erstellt gemäß Artikel 10 der Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG regelmäßig einen Risikovorsorgeplan Strom, in dem entsprechende Krisenszenarien analysiert werden. Der Risikovorsorgeplan ist unter https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/P-R/risikovorsorgeplan-strom-bundesrepublik-deutschland.html abrufbar.

4. In welcher Weise fließen Erkenntnisse aus bundesweiten oder internationalen Ereignissen, insbesondere aus Anschlägen auf Energieinfrastruktur, gegebenenfalls in die Risiko- und Lagebewertungen des Landes ein?

Durch den ständigen Informationsaustausch zwischen Bundes- und Landesbehörden sowie im Rahmen bestehender internationaler Kooperationsstrukturen fließen bundesweite und internationale Gefährdungserkenntnisse in die Lagebewertung für das Land Niedersachsen ein, sofern sie sich mittelbar oder unmittelbar auf die Gefährdungslage auswirken können.

Zudem stimmen sich die niedersächsischen Sicherheitsbehörden in konkreten Einzelfällen im Rahmen der Strafverfolgung sowie Gefahrenabwehr länderübergreifend bilateral ab und tauschen im Rahmen der bestehenden rechtlichen Möglichkeiten Erkenntnisse aus.

Die Auswertungen von Einsatzlagen und Schadensereignissen finden ebenfalls Berücksichtigung und fließen gegebenenfalls in Vorgaben und Konzepte des Landes ein. So sind beispielsweise Erkenntnisse aus der Flutkatastrophe im Ahrtal im Jahr 2021 in die im Jahr 2023 erfolgte Novellierung des Runderlasses Gliederung und Sollstärke von Einheiten des Katastrophenschutzes eingeflossen und wurden bei den technischen Anforderungen für landesseitige Beschaffungsprojekte berücksichtigt.

5. Welche Maßnahmen bestehen auf Landesebene gegebenenfalls zum physischen Schutz kritischer Energieinfrastruktur, insbesondere von Umspannwerken, Netzknoten und Leitstellen?

Der Schutz von KRITIS ist zuvorderst Aufgabe des jeweiligen Betreibers. Im Januar 2023 trat die EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie), die zur Stärkung der Resilienz von KRITIS für alle Mitgliedstaaten beitragen soll, in Kraft. Die Vorschriften der CER-Richtlinie betreffen die physische Widerstandsfähigkeit von KRITIS gegenüber Bedrohungen in Form von etwa Naturkatastrophen, Terroranschlägen oder Sabotage. Die CER-Richtlinie soll durch das KRITIS-Dachgesetz umgesetzt werden, zu dem der Bundesrat am 06.03.2026 zugestimmt hat. Auf Grundlage des Gesetzes sollen Betreibern sektorübergreifend Vorgaben für die physische Sicherheit von KRITIS gemacht werden können.

Niedersachsen setzt sich für eine zeitnahe Umsetzung der CER-Richtlinie ein und begleitet das Umsetzungsvorhaben intensiv und kritisch. Das KRITIS-Dachgesetz bietet jetzt die Voraussetzung für ein höheres Resilienzniveau, auch wenn die beschlossene Fassung in einigen Bereichen hinter den Erwartungen der Länder zurückblieb. Mit Blick auf das anhängige Vertragsverletzungsverfahren besteht ein hoher Umsetzungsdruck. Im Rahmen einer Protokollerklärung zum KRITIS-Dachgesetz wurde jedoch u. a. deutlich gemacht, dass Vorgaben unter Länderbeteiligung in Rechtsverordnungen nachzuschärfen sind,

Leitstellen in Niedersachsen sind grundsätzlich zutrittsgesichert und gegen Ausfälle gehärtet. Hierzu existieren Not- und Ausfallkonzepte, die konkrete Maßnahmen enthalten wie beispielsweise turnusmäßige Funktionsüberprüfungen und die Durchführung von sogenannten „Schwarztests. In der Regel sind Konzepte und Maßnahmen diesbezüglich als Verschlusssache klassifiziert.

Nach Artikel 24 Abs. 1 der Niedersächsischen Verfassung (NV) hat die Landesregierung Anfragen von Mitgliedern des Landtags nach bestem Wissen unverzüglich und vollständig zu beantworten. Die Landesregierung braucht dem Verlangen nicht zu entsprechen, soweit dadurch zu befürchten ist, dass durch das Bekanntwerden von Tatsachen dem Wohl des Landes Nachteile zugefügt werden (Artikel 24 Abs. 3 Satz 1 Alt. 2 NV).

Konkretere Ausführungen zu Maßnahmen und Konzepten könnte Rückschlüsse auf mögliche Angriffsziele zulassen. Insbesondere könnten hierdurch bei einer strategischen Auswertung ein Abgleich stattfinden und künftige Angriffe auf Infrastruktureinrichtungen detaillierter geplant werden. Eine solche Veröffentlichung ist daher geeignet, die Sicherheit der Einrichtungen bzw. Teile der Einrichtungen zu gefährden und mithin dem Wohl des Landes Niedersachsen Nachteile zuzufügen. Deshalb kann die Landesregierung hierzu im Rahmen einer zur Veröffentlichung vorgesehenen Antwort auf eine Kleine Anfrage keine detailliertere Auskunft geben.

6. Welche Rolle übernehmen Polizei, Verfassungsschutz und andere Sicherheitsbehörden beim Schutz kritischer Energieinfrastruktur, und wie ist deren Zusammenarbeit organisiert?

Soweit die Aufgaben der Polizei Niedersachsen betroffen sind, erfordert der Schutz vor Angriffen auf KRITIS sowie vor entsprechenden Bedrohungen eine fortlaufende Bewertung der Sicherheitslage im Sinne eines kontinuierlichen Bedrohungsmanagements. Hierzu gehören die laufende Anpassung der polizeilichen Bekämpfungsstrategien sowie die Weiterentwicklung der daraus abgeleiteten Maßnahmen. Ziel ist es, in enger Abstimmung mit den Betreiberinnen und Betreibern, neue Bedrohungsfor-

men frühzeitig zu erkennen, sicherheitsrelevante Vorkommnisse zu identifizieren und diese beweissicher zu bearbeiten bzw. wirksam abzuwehren. Die Polizei Niedersachsen ermittelt die hierfür bestehenden Handlungsbedarfe fortlaufend und entwickelt diese lageangepasst weiter.

Darüber hinaus übernimmt die Polizei Niedersachsen eine fachkompetente Mitwirkung bei der Aufklärung und Sensibilisierung hinsichtlich der Gefahren im Zusammenhang mit Angriffen oder Bedrohungen auf bzw. gegen KRITIS. Dies umfasst ebenfalls die Sensibilisierung und Stärkung der Resilienz von Mitarbeiterinnen und Mitarbeitern in KRITIS-Einrichtungen sowie die themenorientierte Zusammenarbeit mit weiteren Behörden und Organisationen, insbesondere dem Verfassungsschutz Niedersachsen. Zu diesem Zweck führt die Polizei Niedersachsen anlassbezogen Sicherheitsgespräche mit Betreibern und Verantwortlichen von KRITIS durch. Diese dienen der Stärkung des Gefahrenbewusstseins und der Unterstützung der Sicherheitsausrichtung der Unternehmen. Der gegenseitige Austausch ermöglicht es, sicherheitsrelevante Vorfälle frühzeitig zu identifizieren, zeitnah zu melden und ihnen präventiv vorzubeugen. Etwaigen Erkenntnisdefiziten aufgrund mangelnder Sensibilität oder eingeschränkten Meldeverhaltens seitens der Unternehmen wird so wirksam entgegengewirkt. Ergänzend wird auf die Antwort auf Frage 9 verwiesen.

Seit 2006 besteht mit der sogenannten Global Player Initiative des Bundeskriminalamts ein wechselseitiges Informationsnetzwerk mit deutschen Wirtschaftsunternehmen, darunter solchen, die KRITIS betreiben. Die teilnehmenden Unternehmen werden insbesondere für Phänomenbereiche der PMK sensibilisiert und hinsichtlich sicherheitsgerechter Maßnahmen beraten.

Als Zentralstelle der niedersächsischen Polizei für die Bekämpfung der Cyberkriminalität nimmt die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Niedersachsen (LKA NI) die Funktion einer Ansprechpartnerin für die niedersächsische Wirtschaft wahr - sowohl in präventiven Fragestellungen als auch im Schadensfall. Darüber hinaus ist das LKA NI für komplexe und herausragende Fälle der Cyberkriminalität zuständig, koordiniert die polizeilichen Maßnahmen mit den Polizeidirektionen im Land und arbeitet national wie international mit verschiedenen Ermittlungsbehörden zusammen.

Seitens des Verfassungsschutzes wird nach Übermittlung der KRITIS-Unternehmen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) Kontakt zu den dortigen Sicherheitsverantwortlichen hergestellt, diese aufgesucht und vor Ort zu unterschiedlichsten Sicherheitsfragen (Schwerpunkt Schutz vor Spionage und Sabotage) beraten.

Im Rahmen der Bund-Länder-Gremienarbeit werden bestehende Handlungsempfehlungen fortlaufend überprüft und erforderlichenfalls angepasst.

Ergänzend beschreibt die seit September 2024 veröffentlichte Cybersicherheitsstrategie des Landes Niedersachsen entsprechende Regelungen. Darin wird das abgestimmte Zusammenwirken der beteiligten Behörden hervorgehoben - insbesondere der einschlägigen Arbeitsbereiche des MI, von IT.Niedersachsen, des Verfassungsschutzes Niedersachsen sowie des LKA NI. Der Austausch erfolgt hierzu regelmäßig im Rahmen der Cyberkoordinierungsgruppe.

7. Welche rechtlichen Vorgaben, Standards oder Empfehlungen gelten in Niedersachsen für Betreiber kritischer Energieinfrastruktur zum Schutz ihrer Anlagen?

Vorangestellt ist darauf hinzuweisen, dass die Energieversorgung in Deutschland rein privatwirtschaftlich organisiert ist. Die Energieversorgung in Niedersachsen ist unmittelbar in das bundesweite Energieversorgungssystem eingebunden. Für Betreiber kritischer Energieinfrastruktur gelten somit bundesweite Vorgaben, Standards und Empfehlungen zum Schutz ihrer Anlagen. So sind Netzbetreiber gemäß § 11 Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz zu betreiben und das Netz entsprechend zu verstärken und auszubauen. Für Betreiber kritischer Energieinfrastruktur gelten überdies mit dem von der Bundesnetzagentur kontrollierten IT-Sicherheitskatalog schon jetzt besondere Vorgaben und Standards für die Sicherstellung der IT-Sicherheit.

Im Januar 2023 trat die EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) in Kraft. Sie enthält Vorschriften zur Sicherheit von Netz- und Informationssystemen in Einrichtungen der kritischen Infrastruktur in den Mitgliedstaaten. Die

NIS-2-Richtlinie wird in Deutschland auf Bundesebene als „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ umgesetzt (früherer Titel: „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“). Dieses Bundesgesetz trat am 6. Dezember 2025 in Kraft. Das mit diesem Artikelgesetz novellierte Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) regelt die Aufgaben und Befugnisse des BSI als zentrale deutsche Behörde für Informations- und Cybersicherheit.

Für Einrichtungen des Energiesektors, die in den Anwendungsbereich des BSI-Gesetzes fallen, übernimmt das BSI gemäß § 3 Abs. 1 Ziff. 24 i. V. m. § 40 BSI-Gesetz die Aufgaben als zentrale Stelle für die Sicherheit in der Informationstechnik besonders wichtiger Einrichtungen einschließlich der Betreiber kritischer Anlagen. Den betreffenden Einrichtungen bietet das BSI Unterstützungs- und Beratungsangebote. Zudem ist das BSI für diese Einrichtungen zentrale Meldestelle für Sicherheitsvorfälle und übt aufsichtsbehördliche Funktion aus.

Die Betreiber von Einrichtungen im Energiesektor, die in den Anwendungsbereich des BSI-Gesetzes und gegebenenfalls der darauf basierenden Rechtsverordnungen gemäß § 56 BSI-Gesetz fallen, haben ein systematisches Informationssicherheitsmanagement einschließlich Risikomanagement sowie ein Notfallmanagement zu betreiben. Die Angemessenheit des Informationssicherheitsmanagements kann beispielsweise auf Basis der internationalen Normenreihe ISO 27001 ff. oder der darauf basierenden IT-Grundschutz-Methodik auf Grundlage der BSI-Standards nachgewiesen werden, insbesondere der BSI-Standards 200-1 bis 200-4. Diese Methodik samt Standards wird aktuell fortgeschrieben. Zudem sind diese Einrichtungen zur Meldung gravierender Sicherheitsvorfälle an das BSI verpflichtet.

Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

8. In welchem Umfang erfolgt gegebenenfalls eine Überprüfung oder Begleitung der Betreiber durch das Land hinsichtlich der Umsetzung von Schutzmaßnahmen?

9. Wie ist die Zusammenarbeit zwischen Landesregierung und Betreibern kritischer Energieinfrastruktur organisiert?

Die Fragen 8 und 9 werden aufgrund des sachlichen Zusammenhangs gemeinsam beantwortet.

Der Fachbereich Wirtschaftsschutz beim Niedersächsischen Verfassungsschutz berät seit vielen Jahren KRITIS-Unternehmen in Niedersachsen u. a. zu den Themen Resilienz, Redundanz und Lieferkettenabhängigkeiten und stellt die Kontakte zu den Sicherheitsbereichen der Unternehmen her. Diese Kontakte werden mit dem LKA Niedersachsen und Abteilung 7 des MI geteilt. Sofern konkrete Warnmeldungen oder Hinweise vorliegen, werden diese an die Security-Manager der Unternehmen gesteuert.

Weiterhin werden durch das MI regelmäßig KRITIS-Tagungen für Security-Manager der Unternehmen durchgeführt. Diese Veranstaltungen dienen der Weitergabe von Informationen, dem gemeinsamen Austausch sowie der Vernetzung.

Überdies findet ein regelmäßiger Austausch des Niedersächsischen Ministeriums für Umwelt, Energie und Klimaschutz mit Netzbetreibern im Rahmen der Task Force Energiewende, u. a. zur beschleunigten Umsetzung des Netzausbaus und somit zur Erhöhung der Systemstabilität des Stromnetzes in Niedersachsen, was auch einen zentralen Beitrag zur Stärkung der Resilienz von kritischer Energieinfrastruktur leistet.

Im Übrigen wird auf die Antwort zu Frage 6 verwiesen

10. Welche Anforderungen stellt das Land gegebenenfalls an Betreiber hinsichtlich Risikomanagement, Schutzkonzepten und Meldewegen?

Die Landesregierung ist in die Melde- und Kommunikationswege der Stromnetzbetreiber für den Krisenfall eingebunden.

Die Polizei Niedersachsen bietet insbesondere Beratung und Unterstützung an. Mit Blick auf die Meldewege werden Betreiberinnen und Betreiber fortlaufend hinsichtlich einer niedrigschwelligen, zeitnahen Mitteilung von Sicherheitsvorfällen bzw. Verdachtsfällen sensibilisiert. Dies dient zum einen einer wirksamen Schadensbegrenzung, zum anderen aber auch einer frühestmöglichen Initiierung von Ermittlungsmaßnahmen, sofern im Einzelfall ein strafrechtlich relevanter Hintergrund anzunehmen ist.

§ 18 des KRITIS-Dachgesetzes sieht Vorfallsmeldungen durch Betreiber an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe vor. Die Weitergabe der Vorfallsmeldungen an die Länder wird der Bund gemeinsam mit den Ländern in einer Verordnung regeln.

Im Übrigen wird auf die Antworten zu den Fragen 5, 6 sowie 8 und 9 verwiesen.

11. Inwiefern unterstützt das Land Betreiber kritischer Energieinfrastruktur gegebenenfalls bei der Stärkung ihrer Resilienz, etwa durch Beratung, Koordination oder Fördermaßnahmen?

Es wird auf die Antworten zu den Fragen 6 sowie 8 und 9 verwiesen.

12. Welche Schlussfolgerungen zieht die Landesregierung aus aktuellen sicherheitspolitischen Entwicklungen für den Schutz der Stromversorgung in Niedersachsen?

Mit Blick auf die sicherheitspolitischen Entwicklungen kommt der Stärkung der Resilienz kritischer Infrastrukturen sektorübergreifend und damit auch in der Stromversorgung eine immer stärkere Bedeutung zu. Vor diesem Hintergrund erwartet die Landesregierung von den Stromnetzbetreibern entsprechend ihrer gesetzlichen Verpflichtungen die Robustheit des Stromnetzes gegenüber Störungen fortlaufend zu evaluieren und zu stärken.

Die Polizei Niedersachsen hat im Rahmen des Notfallmanagements jüngst die Leitlinie Notfallmanagement aktualisiert und auf aktuelle Herausforderungen sowie Bedrohungen der Gegenwart angepasst.

Darüber hinaus stehen die niedersächsischen Polizeibehörden in einem regelmäßigen und anlassbezogenen Austausch mit den regionalen Stromversorgungsunternehmen, um etwaige zusätzliche Schutzmaßnahmen zu prüfen und abzustimmen.

Im Übrigen wird auf die Antworten zu den Fragen 6 sowie 8 und 9 verwiesen.

13. Plant die Landesregierung Anpassungen bestehender Konzepte, rechtlicher Rahmenbedingungen oder organisatorischer Strukturen, um den Schutz kritischer Energieinfrastruktur zu stärken (bitte gegebenenfalls die einzelnen geplanten Maßnahmen aufführen)?

Es wird auf die Antworten zu den Fragen 6 und 12 verwiesen.

Aufgrund von Transparenzpflichten (z. B. Bundes-Immissionsschutzgesetz) sind Unternehmen verpflichtet, teilweise sicherheitsrelevante Informationen zu veröffentlichen. Eine Verringerung dieser Veröffentlichungspflichten wäre dem Schutz von KRITIS förderlich. Da die meisten derartigen Vorschriften dem Bundesrecht unterliegen, ist das Bundesministerium für Inneres (BMI) gefordert, die entsprechenden Regelungen zu überprüfen und gegebenenfalls anzupassen. Eine entsprechende Initiative zur Überprüfung und Anpassung der gesetzlichen Bestimmungen ist bereits über die Bund-Länder-Gremien erfolgt und seitens des BMI in der Befassung.

14. Welche zusätzlichen Maßnahmen oder Investitionen sind hierzu gegebenenfalls vorgesehen?

Wie bereits in der Antwort zu Frage 7 erläutert, ist die Energieversorgung in Deutschland privatwirtschaftlich organisiert mit entsprechenden Zuständigkeiten und Verantwortlichkeiten im Kontext der Krisenprävention und des Krisenmanagements. Konkrete Maßnahmen und Investitionen zur Stärkung der Resilienz des Stromnetzbetriebs obliegen somit primär den Netzbetreibern.

Bezüglich der weiteren Maßnahmen wird auf die Antworten zu den Fragen 6 und 12 verwiesen.