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

Anfrage der Abgeordneten Jonas Pohlmann, Verena Kämmerling und Andre Bock (CDU)

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

Wie kann die Resilienz der kritischen Infrastruktur Niedersachsens gestärkt werden?

Anfrage der Abgeordneten Jonas Pohlmann, Verena Kämmerling und Andre Bock (CDU), eingegangen am 01.07.2025 - Drs. 19/7660,
an die Staatskanzlei übersandt am 07.07.2025

Antwort des Niedersächsischen Ministeriums für Inneres, Sport und Digitalisierung namens der Landesregierung vom 11.08.2025

Vorbemerkung der Abgeordneten

Die Stärkung kritischer Infrastruktur rückt sowohl auf europäischer als auch auf Bundesebene aufgrund zunehmender geopolitischer Spannungen in den Vordergrund.[1]

Auf Landesebene wird die Landesregierung in dem von den Fraktionen der SPD und Bündnis 90/Die Grünen eingereichten Entschließungsantrag „Gemeinsam die Resilienz Niedersachsens stärken“ (Drs. 19/6284) unter Nummer 3 aufgefordert, „zu prüfen, wie ein Kommunikationssystem für den Fall eines großflächigen Stromausfalls, eines IT-Ausfalls oder Cyberangriffs in Zusammenarbeit mit den Kommunen entwickelt werden kann.“

Vorbemerkung der Landesregierung

Kritische Infrastrukturen (kurz: KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Der Bund hat sich mit den Ländern im Jahr 2011 auf die Einteilung von neun KRITIS-Sektoren verständigt. Dies stellt zwar keine gesetzliche Regelung dar, dennoch prägt sie das Verständnis der Landesregierung hinsichtlich der Frage der Definition von kritischen Infrastrukturen. Im Zuge der Novellierung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) kam 2021 mit der Siedlungsabfallentsorgung ein zehnter Sektor hinzu. Die zehn Sektoren lauten: Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik & Telekommunikation, Siedlungsabfallentsorgung, Medien und Kultur, Transport und Verkehr, Wasser und Staat und Verwaltung.

Diese Sektoren decken sich jedoch nicht vollständig mit den Sektoren, die sich aus § 2 Abs. 10 BSI-Gesetz ergeben und in der Folge in den Anwendungsbereich des BSI-Gesetzes fallen. Die Sektoren Staat und Verwaltung sowie Medien und Kultur zählen zwar zu den KRITIS-Sektoren nach der o. g. KRITIS-Definition, unterliegen aber nicht der Regulierung durch das BSI-Gesetz. Die gesetzlichen Mindestanforderungen, die sich im Wesentlichen aus § 8 a BSI-Gesetz ergeben (z. B. eine regelmäßige Risikoanalyse auf Basis des Stands der Technik, die Beschreibung technischer und

[1] https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html und https://www.vdi-nachrichten.com/technik/informationstechnik/schutz-kritischer-infrastruktur-im-fokus-der-politik/

organisatorischer Maßnahmen oder eine Echtzeit-Erkennung und Abwehr von IT-Sicherheitsvorfällen) müssen daher von dem Sektor Staat und Verwaltung nicht aufgrund des BSI-Gesetzes erfüllt werden. Der niedersächsische Gesetzgeber hat über § 5 a Abs. 1 Nr. 2, Abs. 5 Niedersächsisches Katastrophenschutzgesetz (NKatSG) der Landesregierung jedoch eine Verordnungsermächtigung gegeben, um landesspezifisch KRITIS zu definieren. Mit Blick auf die anstehende nationale Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) wurde hiervon bislang noch kein Gebrauch gemacht; die Umsetzung durch den Bund bleibt abzuwarten.

Für KRITIS, die in den Anwendungsbereich des BSI-Gesetzes fallen, also sowohl in einem der Sektoren des BSI-Gesetzes tätig sind, als auch den erforderlichen Schwellenwert überschreiten, der in der BSI-Kritisverordnung beschrieben wird, übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß § 3 Abs. 1 Ziff. 17 BSI-Gesetz die Aufgaben nach den §§ 8 a bis 8 c und 8 f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse. Auch kommunale Eigenbetriebe sowie Unternehmen, die sich in öffentlicher Hand befinden, können KRITIS i. S. des BSI-Gesetzes sein mit der Folge, dass das BSI Unterstützungs- und Beratungsangebote bietet. Dies ist beispielsweise bei größeren Wasserwerken, Stadtwerken oder kommunalen Krankenhäusern möglich.

Unabhängig von der Nicht-Regulierung des Sektors Staat und Verwaltung durch das BSI-Gesetz unterstützt die Landesregierung bei der Härtung der Resilienz kritischer Verwaltungsprozesse. Dies gilt sowohl für Verwaltungsprozesse der Landesbehörden als auch für die kommunale Verwaltung.

Im Januar 2023 traten zudem die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) sowie die CER-Richtlinie, die zur Stärkung der Resilienz von Kritischen Infrastrukturen für alle Mitgliedstaaten beitragen sollen, in Kraft. Während die Vorschriften der CER-Richtlinie die physische Widerstandsfähigkeit von KRITIS gegenüber Bedrohungen in Form von etwa Naturkatastrophen, Terroranschlägen oder Sabotage betreffen, enthält die NIS-2-Richtlinie Vorschriften zur Sicherheit von Netz- und Informationssystemen.

Die NIS-2-Richtlinie soll in Deutschland als NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt werden. Eine Länderbeteiligung hat auf Grundlage des vorliegenden Referentenentwurfs bereits stattgefunden. Das Land Niedersachsen hat seine rechtlichen Umsetzungsverpflichtungen bereits vollständig erfüllt. Am 29.10.2024 hat die Landesregierung den Gemeinsamen Runderlass „Umsetzung der NIS-2-Richtlinie in Niedersachsen (NIS2UmsRdErl)“ erlassen sowie das Ministerium für Inneres, Sport und Digitalisierung (MI) als zuständige Behörde für Cybersicherheit i. S. von Artikel 8 Abs. 1 NIS-2-Richtlinie und die Zentralstelle für Informationssicherheit (N-CERT) als Computer-Notfallteam (CSIRT) i. S. von Artikel 10 Abs. 1 NIS-2-Richtlinie benannt. Besonders kritische Teile der unmittelbaren Landesverwaltung sind verpflichtet, Risikomanagementmaßnahmen zu treffen, um ihre Resilienz zu stärken. Auf Bundesebene soll die CER-Richtlinie durch ein KRITIS-Dachgesetz umgesetzt werden.

Abgesehen von den o. g. Vorschriften gibt es in Deutschland bislang kein sektoren- und gefahrenübergreifendes Gesetz zum Schutz von KRITIS. Gesetzliche Regelungen mit Bezug zum physischen Schutz spezifischer Kritischer Infrastrukturen finden sich vereinzelt und in unterschiedlicher Regelungstiefe in Fachgesetzen. Darüber hinaus fördern weitere gesetzliche Regelungen, Normen und Standards mittelbar auch den physischen KRITIS-Schutz, wie etwa bautechnische Vorschriften.

Die Landesregierung ist dem Beschluss des IT-Planungsrates Bund/Länder vom 03.11.2023 gefolgt und hat keinen Gebrauch von der fakultativen Einbeziehung der Kommunalverwaltungsebene gemacht. Insofern sind die Kommunen in ihrer Kernverwaltung von den Vorgaben der NIS-2-Richtlinie nicht betroffen. Die Nicht-Einbeziehung bezieht sich jedoch lediglich auf Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 6 Nr. 35 der NIS-2-Richtlinie. Sowohl kommunale Unternehmen als auch kommunale Eigenbetriebe werden in den Anwendungsbereich der Richtlinie fallen, sofern sie in einem der Sektoren des Anhangs I und II der NIS-2-Richtlinie tätig sind (u. a. Energie, Verkehr, Gesundheitswesen, Trinkwasser, Abwasser und Abfallwirtschaft) und die sogenannte Size-Cap-Rule erfüllen (mind. 50 Beschäftigte und/oder mind. 10 Millionen Euro Jahresumsatz). Ein wesentlicher Teil der kritischen Aufgaben der Daseinsvorsorge einer Kommune wird dadurch von Cybersicherheitsmindestanforderungen betroffen sein. Diese Einrichtungen werden über Bundesrecht reguliert. Dies entspricht der derzeitigen Rechtslage, sofern Kommunen KRITIS betreiben.

Im Ergebnis ist vor diesem Hintergrund nicht jede Verwaltungseinrichtung auf kommunaler Ebene als KRITIS zu betrachten.

In der vorliegenden Kleinen Anfrage zur schriftlichen Beantwortung findet der Begriff „Resilienz“ zentrale Verwendung. Im Zusammenhang der Cybersicherheit wird der Begriff als Widerstandsfähigkeit gegenüber entsprechenden Cyberbedrohungen verstanden, welche durch Maßnahmen zur Prävention, Detektion und Reaktion sichergestellt wird.

1. Inwiefern unterstützt die Landesregierung gegebenenfalls die Kommunen bei der Umsetzung von Maßnahmen zur Verbesserung der Resilienz der lokalen kritischen Infrastrukturen?

Der Beantwortung der Frage wird vorangestellt, dass die Landesregierung allen niedersächsischen Kommunen gleichermaßen Unterstützungsangebote zur Verbesserung der Resilienz bereitstellt. Seitens der Landesregierung wird hierbei nicht differenziert, ob Geschäftsbereiche der einzelnen Kommune unter Kritische Infrastrukturen fallen oder nicht (siehe auch die Vorbemerkung der Landesregierung).

Die Landesregierung hat die Kommunen mit kostenfreien Schulungen zum Business Continuity Management (BCM) von April 2024 bis Mai 2025 unterstützt. Diese Managementdisziplin beschäftigt sich mit der Implementierung und dem Aufbau eines strategischen Notfallmanagements und dient der Identifikation kritischer Geschäftsprozesse im Not- und Krisenfall. Die Schulungen basieren auf etablierten Standards wie dem BSI-Standard 200-4 und weiteren IT-Sicherheitsframeworks, um Methodik und Anwendung eines Notfallmanagements zu vermitteln. Unter den Teilnehmenden befanden sich ebenfalls Beschäftigte aus dem Landesdienst und von kommunalen IT-Dienstleistern. Darüber hinaus wird seit März 2025 ein Projekt mit niedersächsischen Kommunen durchgeführt, um kritische Geschäftsprozesse zu identifizieren und deren Absicherung voranzutreiben. Im Fokus stehen Prozesse, die eine gemeinsame, in der Regel digitale, Schnittstelle zwischen Land und Kommune haben. Diese Maßnahme unterstützt die Absicherung der digitalen Dienste, um sicherzustellen, dass diese auch in Notfall- und Krisensituation verfügbar sind.

Zur Stärkung der Resilienz gegen Cyberangriffe hat das MI den niedersächsischen Kommunen in den vergangenen Jahren außerdem die Durchführung von Cybersicherheitsanalysen als Unterstützungsmöglichkeit angeboten. Mithilfe einer Cybersicherheitsanalyse kann ermittelt werden, ob die bereits getroffenen Schutzmaßnahmen eine ausreichende Widerstandfähigkeit gegen Cyberangriffe gewährleisten. Dazu wurden mit den interessierten Kommunen die wesentlichen technischen und organisatorischen Anforderungen an eine angemessene Absicherung gegen verschiedene Bedrohungen untersucht und fachlich bewertet. Diese Leistung war für die Kommunen kostenfrei und erfolgte auf freiwilliger Basis. Von dem Angebot, welches zum Herbst 2024 auslief, konnten seit 2022 insgesamt 228 Kommunen aus allen Gemeindearten in Niedersachsen profitieren. Das Land Niedersachsen hat insgesamt rund 1,5 Millionen Euro für dieses Projekt investiert.

In den Handlungsfeldern Prävention, Detektion und Reaktion stellt das Niedersächsische Computer Emergency Response Team (N-CERT) zusätzlich seine Warn- und Informationsdienste auch den Kommunen zur Verfügung. Derzeit nehmen rund 160 Kommunen diesen Dienst in Anspruch. Zudem können Beratungsleistungen des N-CERT, etwa bei der Konzeption von Maßnahmen der IT-Sicherheit oder auch akut im Rahmen der Bewältigung von Sicherheitsvorfällen, in Anspruch genommen werden. In regelmäßigen Treffen mit den IT-Fachkräften in den Kommunen wird der Informationsaustausch gefördert und aktiv Feedback zu den Leistungen des N-CERT eingeholt. Mit einem ebenfalls für die Kommunen kostenlosen Workshop-Angebot weitet das N-CERT seine Leistungen für den kommunalen Bereich weiter aus. Mit ersten interessierten Kommunen ist eine Informationsplattform über Schadsoftware und Cyberangriffe (Malware Information Sharing Platform, MISP) für den kommunalen Bereich in Erprobung, sodass dieses Angebot künftig allen Kommunen in Niedersachsen zur Verfügung gestellt werden kann. Im Rahmen des Kommunalen IT-Sicherheitsbündnisses Niedersachsen (KITSIN) arbeitet das N-CERT eng mit den kommunalen Einrichtungen in Niedersachsen zusammen, beispielsweise finden zweimal jährliche gemeinsame Arbeitstreffen statt.

Das Land befindet sich derzeit in Gesprächen mit den kommunalen IT-Dienstleistern über eine engere Kooperation beim Betrieb eines Security Operation Center (SOC) und die Nutzung einer gemeinsamen Softwarelösung zur automatisierten Identifizierung von Schadsoftware und Abwehrmaßnahmen. Es ist geplant, auf dieser Basis ein landesweites Lagebild über Gefährdungen aus dem Netz aufzubauen.

Die Landesregierung beabsichtigt, ihre Maßnahmen zur Verbesserung der gesamtstaatlichen Cybersicherheit - unter Einbeziehung der Kommunen - bedarfsgerecht weiterzuentwickeln und die Koordinierung und Steuerung durch das übergreifende Cybersicherheitsmanagement im MI auszubauen.

Der Bereich Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes unterstützt Kommunen - nach Anfrage - mit bekannten Präventionsangeboten (Beratung, Vorträge) und durch Teilnahme an lokalen Sicherheitszirkeln. Außerdem werden Tagungen (Informationsveranstaltungen) veranstaltet, an welchen auch Vertreter aus den öffentlichen Bereichen teilnehmen können.

Die Landesregierung und die kommunalen Spitzenverbände haben am 24.03.2025 den sogenannten Pakt für Kommunalinvestitionen geschlossen. Mit diesem werden den Kommunen u. a. 600 Millionen Euro für kommunale Investitionen bereitgestellt. Eine Einschränkung auf bestimmte Investitionsbereiche ist nicht vorgesehen. Die zur Verfügung stehenden Mittel können somit grundsätzlich auch für Investitionen in die Kritische Infrastruktur verwendet werden.

Im Bereich der Wasserversorgung setzt das Wassersicherstellungsgesetz (WasSG) des Bundes den Rahmen für die Trinkwassernotversorgung in Deutschland. Der Bund übernimmt in diesem Zusammenhang bestimmte Kosten wie z. B. Brunnenneubau. Die Bundesländer arbeiten hier im Rahmen der Bundesauftragsverwaltung; darüber hinaus findet durch das Land keine konkrete Finanzierung von kommunalen Maßnahmen zur Wassersicherstellung statt.

Weiterhin finden Gespräche unter Beteiligung des Ministeriums für Wissenschaft und Kultur (MWK) und MI mit dem Landesfeuerwehrverband und Akteuren der regionalen Kulturförderung (Arbeitsgemeinschaft der Landschaften und Landschaftsverbände [ALLviN]) mit dem Ziel statt, lokale bzw. regionale Notfallverbünde in Niedersachsen, an denen regelmäßig auch Kultureinrichtungen unterschiedlicher Trägerschaft beteiligt sind, zu vernetzen und zu unterstützen.

Im Rahmen seiner Zuständigkeit für die Umsetzung des Ernährungssicherstellungs- und -vorsorgegesetzes (ESVG) führt das Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz (ML) außerdem regelmäßig (i. d. R. jährlich) Dienstbesprechungen mit den zuständigen Kommunen auf Ebene der Landkreise und kreisfreien Städte durch. Dabei werden auch Fragestellungen zur Kritischen Infrastruktur Ernährung, z. B. mit Bezug zum geplanten KRITIS-Dachgesetz, diskutiert.

Im Rahmen des vom Bundesministerium für Forschung, Technologie und Raumfahrt geförderten und vom ML durchgeführten Projektes Kritische Infrastruktur Ernährung: Erarbeitung innovativer Entscheidungs- und Kooperationssysteme für die Ernährungsnotfallvorsorge (KRITIS-ENV) sind darüber hinaus elf niedersächsische Kommunen als assoziierte Partner eingebunden.

Seit der COVID Pandemie wurde erheblich in die Digitalisierung der kommunalen Gesundheitsämter investiert. Dies erfolgte insbesondere im Rahmen des sogenannten Paktes für den Öffentlichen Gesundheitsdienst, für den EU-Mittel im Rahmen des Deutschen Aufbau- und Resilienzplans (DARP) verwendet wurden. Ein wichtiges Ziel war die Erhöhung der digitalen Reife der Gesundheitsbehörden auch im Bereich der Informationssicherheit, wozu beispielsweise auch das Business Continuity Management zählt, also die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit bei eintretenden Störungen. Die Landesregierung hat die Kommunen in diesem Prozess umfänglich unterstützt. insbesondere durch die Erstellung einer Digitalstrategie und eines Schulungskonzeptes sowie durch den Betrieb einer Geschäftsstelle, die die Aktivitäten landesweit koordiniert und unterstützt.

Am Landesgesundheitsamt (NLGA) wurden in diesem Zusammenhang zusätzliche digitale Tools entwickelt und eingeführt, die in Krisensituationen Unterstützung liefern können, z. B. ein Chat- und Voicebot mit dem ein erhöhtes Aufkommen von Anfragen von Bürgerinnen und Bürgern in einer Krisensituation effizient bearbeitet werden kann.

Des Weiteren führt die Hafensicherheitsbehörde Niedersachsen für Häfen und Hafenanlagen, die im internationalen Seeverkehr eingebunden sind, Risikobewertungen gemäß dem Niedersächsischen Hafensicherheitsgesetz durch. Im Jahr 2024 wurden diese Risikobewertungen überarbeitet und im

Hinblick auf Cyberkriminalität, Drohnensichtungen sowie Ausspähungen im Zusammenhang mit Spionage/Sabotage nachgeschärft. Risiken in diesen Bereichen werden identifiziert und bewertet, wonach die Unternehmen diesen aufgedeckten Risiken durch geeignete Maßnahmen begegnen müssen. Ebenfalls werden zum Thema Infiltration der Nordseehäfen durch die organisierte Kriminalität (INOK) Aufklärungs- und Sensibilisierungsveranstaltungen in Kooperation mit der Polizei Niedersachsen angeboten.

Eine integrierte Sicherheitsvorsorge in Bezug auf die Infrastruktur eines Hafens findet sich in den durch die Hafensicherheitsbehörde Niedersachsen erstellten Gesamthafenplänen gemäß RL 2005/65/EG wieder. Das Ziel der RL 2005/65/EG ist es, die Sicherheitskonzepte von Polizei, Feuerwehr und Katastrophenschutz im Kontext der Seehäfen zusammenzuführen.

2. Wie wird die ressortübergreifende Zusammenarbeit im Bereich der Resilienz kritischer Infrastrukturen auf Landesebene zwischen dem Ministerium für Inneres und Sport und dem Ministerium für Umwelt, Energie und Klimaschutz geregelt? Welches Ministerium besitzt welche Befugnisse bzw. Verantwortungen?

Im MI wurde die koordinierende Stelle für KRITIS gebildet. Hier sitzt auch die Geschäftsstelle für den Interministeriellen Arbeitskreis zum Schutz Kritischer Infrastrukturen, an dem alle obersten Landesbehörden beteiligt sind. Weiter finden alle vier Wochen Besprechungen zum jeweiligen aktuellen Status in den KRITIS-Sektoren statt. In diesen Besprechungen wird sich zur Lage in den KRITIS, z. B. in Bezug auf etwaige Störungen, ausgetauscht. Das Ministerium für Umwelt, Energie und Klimaschutz (MU) erstellt hierfür regelmäßig Statusmeldungen zur Lage in den KRITIS-Sektoren Energie, öffentliche Abwasserbeseitigung und Siedlungsabfallentsorgung.

Neben diesen ressortübergreifenden Austauschformaten finden anlassbezogen auch bilaterale Gespräche auf Arbeitsebene zwischen dem MU und dem MI statt.

Das MI steht ferner mit allen Ministerien und der Staatskanzlei im Austausch, um die gesamtstaatliche Cybersicherheitsarchitektur weiter auszubauen und dabei auch kritische Einrichtungen in Niedersachsen über die Zuständigkeiten des BSI hinaus zu unterstützen. Diese Bestrebungen der Landesregierung beinhalten auch eine organisatorische Konsolidierung und einen Ausbau des übergreifenden Cybersicherheitsmanagements im MI.

3. Welche Zuständigkeiten und Verantwortungen haben jeweils der Bund, das Land, die Landkreise sowie die Städte und Gemeinden in diesem Bereich?

Voranzustellen ist, dass der Schutz von KRITIS zuvorderst in der Verantwortung der jeweiligen Betreiber liegt.

Der Bund ist für die Umsetzung der CER-Richtlinie und die übergreifende KRITIS-Gesetzgebung zuständig. Zum KRITIS-Dachgesetz hat die Landesregierung bislang verschiedene Referentenentwürfe des Bundes erhalten, zu denen die Landesregierung kritisch Stellung genommen und Überarbeitungsbedarfe aufgezeigt hat. Da bislang nur Referentenentwürfe vorliegen, zu denen noch weiterer Abstimmungsbedarf besteht, entfalten diese noch keine Rechtswirkungen.

In Niedersachsen wurde darüber hinaus mit § 5 a NKatSG bereits frühzeitig der KRITIS-Schutz normiert. Durch das Inkrafttreten der CER-Richtlinie und die notwendige Umsetzung durch den Bund über das geplante KRITIS-Dachgesetz musste eine weitere Ausgestaltung der Norm bislang zurückgestellt werden.

Für den Bereich Cybersicherheit wird auf die Vorbemerkung der Landesregierung und die Antwort zu Frage 1 verwiesen.

In staatlichen Angelegenheiten unterliegen die Medizinische Hochschule Hannover (MHH) und die Universitätsmedizin Göttingen (UMG) der Fachaufsicht des MWK. Die MHH unterliegt auch in Angelegenheiten der Selbstverwaltung der Rechtsaufsicht des MWK. An der UMG übt die Stiftung durch den Stiftungsausschuss UMG die Rechtsaufsicht über die Hochschule aus.

MHH und UMG sind zentrale Einrichtungen im Krisenfall. Sie verfügen über Krankenhausalarm- und Einsatzpläne.

Nach aktuellem Status quo gibt es für den Bereich der Stärkung der Resilienz im Eisenbahnbereich keine Zuständigkeiten für die Länder und Kommunen. Nach erfolgtem Lückenschluss durch das „KRITIS-Dachgesetz“ soll das Eisenbahn-Bundesamt für den weitüberwiegenden Teil der deutschen Eisenbahninfrastruktur und der darauf erbrachten Verkehrsleistungen als sektorspezifische Aufsichtsbehörde mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zusammenarbeiten. Die Länder werden diese Aufgaben für die Eisenbahninfrastruktur der nicht zum DB-Konzern gehörenden Eisenbahninfrastrukturen und der darauf erbrachten Verkehrsleistungen übernehmen.

Niedersachsen hat bezüglich der Anlagen und der Verkehrsleistungen der Eisenbahnen des Bundes und der Eisenbahnverkehrsunternehmen in der Aufsicht des Eisenbahn-Bundesamtes keine Zuständigkeiten.

In Niedersachsen werden jedoch rund 1 000 km Eisenbahninfrastruktur betrieben, die nicht zum Netz der bundeseigenen DB InfraGO AG gehören und der Aufsicht des Landes unterliegen. Aufgrund ihrer regionalen Bedeutung werden diese Eisenbahninfrastrukturen voraussichtlich nicht von den Vorgaben zum besonderen Schutz der kritischen Infrastruktur nach dem „KRITIS-Dachgesetz“ erfasst.

Dessen ungeachtet, misst die Landesregierung auch dem Schutz dieser regional bedeutsamen Eisenbahninfrastrukturen eine hohe Bedeutung zu. Daher wird im Rahmen der Aufsicht über diese Eisenbahninfrastrukturen darauf hingewirkt, dass die Eisenbahninfrastrukturen möglichst resilient gegen äußere Störungen sind. Aufgrund ihres Infrastrukturstandards weisen diese Eisenbahninfrastrukturen jedoch bereits einen hohen Grad an Resilienz insbesondere zumindest gegen Cyberattacken auf und verfügen über in der Praxis eingeübten Rückfallebenen, die auch im Falle des Ausfalls von digitalen Systemen einen sicheren und stabilen Betrieb ermöglichen.

Aufgaben für die Kommunen sind im Eisenbahnbereich nicht vorgesehen.

4. Hat sich die Landesregierung bereits der dritten Forderung aus dem Antrag in der Drucksache 19/6284 gewidmet? Wenn nicht, warum (noch) nicht? Wenn ja, welche Maßnahmen wurden zu diesem Zweck gegebenenfalls eingeleitet?

Zur Sicherstellung der Kommunikationsfähigkeit zwischen der obersten, der oberen und den unteren Katastrophenschutzbehörden sowie der Führungszüge Land beschafft das Landesamt für Brand- und Katastrophenschutz im Auftrag des MI ein verlässliches und hochverfügbares System zur Übertragung von Sprache und Daten („Katastrophenschutznotfallnetz Niedersachsen [KaNN]“) via Satelliten. Die zuständige zentrale Beschaffungsstelle wurde im vierten Quartal 2024 mit der Durchführung des Vergabeverfahren beauftragt.

Bereits aus den Mitteln des Ad-hoc-Pakets zur Stärkung des Katastrophenschutzes in 2022 wurden den unteren Katastrophenschutzbehörden Mittel u. a. zur Ertüchtigung ihrer Fernmeldezentralen zur Verfügung gestellt. In vielen Fällen wurde hiervon u. a. Satellitentelefone erworben.

5. Wieviel wurde seit dem Jahr 2023 in die Stärkung der Resilienz kritischer Infrastrukturen seitens der Landesregierung investiert (bitte nach Bereichen aufschlüsseln)?

Wie bereits ausgeführt, sind die Betreiberinnen und Betreiber selbst für Investitionen in die Stärkung der Resilienz von KRITIS verantwortlich.

Zur Beantwortung dieser Frage werden zunächst alle Mittel zur Stärkung der digitalen Resilienz im Sektor Staat und Verwaltung aufgeführt, ohne dabei zu unterscheiden, ob es sich dabei um kritische Infrastrukturen handelt oder nicht (siehe auch die Vorbemerkung der Landesregierung und die Beantwortung der Frage 1).

Investitionen für die Themen BCM und Cybersicherheit ab 2023 stellen sich wie folgt dar:

Jahr	Bereich	Art	Finanzielle Mittel
2023	Staat und Verwaltung Kommunen	Unterstützung beim BCM	11.210,00 Euro
2023	Staat und Verwaltung Kommunen	Stärkung der Cybersicherheit	113.760,00 Euro
2023	Staat und Verwaltung Landesverwaltung	Unterstützung beim BCM	79.030,00 Euro
2024	Staat und Verwaltung Kommunen	Unterstützung beim BCM	24.240,00 Euro
2024	Staat und Verwaltung Kommunen	Stärkung der Cybersicherheit	532.305,39 Euro
2024	Staat und Verwaltung Landesverwaltung	Unterstützung beim BCM	2.503.666,00 Euro

Ausgaben des Katastrophenschutzes haben oftmals auch einen Nutzen zur Stärkung der Resilienz Kritischer Infrastrukturen. Im Bereich Katastrophenschutz wurden seit 2023 etwa 5,3 Millionen Euro verausgabt, die mittelbar oder unmittelbar die Resilienz Kritischer Infrastrukturen stärken.

Im Haushaltsplan und in der -führung des MU wird nicht gesondert nach dem Kriterium „Resilienz“ oder „kritische oder nicht-kritische Infrastruktur“ bei den investiven Maßnahmen unterschieden.

Mittel zur Stärkung der Resilienz Kritischer Infrastrukturen werden im Einzelplan des MWK nicht explizit ausgewiesen. Im Rahmen der Förderung des Kulturrats Oldenburg sind im Haushaltsjahr 2024 für die Oldenburger Kultureinrichtungen Mittel in Höhe von knapp 21 500 Euro für die Erstausstattung des Notfallverbundes Oldenburg bewilligt worden (u. a. mit einem Stromerzeuger, diverse Gitterwagen und Faltpavillons).

Gemäß des IT-Sicherheitsgesetzes vom 13.12.2017 fallen Krankenhäuser mit einer stabilen Fallzahl von deutlich mehr als 30 000 vollstationären Fällen dauerhaft unter die Kriterien der BSI-KRITISV als Betreiber einer kritischen Infrastruktur. Nach § 8 a BSI-Gesetz sind diese Häuser 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.“ Aus dem Strukturfond vom Bund und dem Land Niedersachsen wurden in dem Jahr 2023 hierfür insgesamt 3 Millionen Euro bereitgestellt.

Im Bereich der Seehäfen wurden Anstrengungen der Landesregierung zur Stärkung der Resilienz unternommen. Die Port Authority führt entsprechende Maßnahmen im Rahmen ihres gesetzlichen Auftrages durch.

Seit 2022 wurde die Kooperation zwischen dem Geschäftsbereich des MI und dem Geschäftsbereich des MW durch Schaffung einer gemeinsamen Hafensicherheitsbehörde, verbunden mit einer personellen Stärkung, seit dem 01.10.2024 unter Leitung der Landesbehörde für Straßenbau und Verkehr, gegründet. Mit dem Haushaltsplan 2024 wurden rund 501 Tausend Euro im Landeshaushalt für insgesamt acht zusätzliche Vollzeiteinheiten veranschlagt. Davon entfallen vier zusätzliche Vollzeiteinheiten auf den Geschäftsbereich des MW mit einem Personalkostenbudget i. H. v. 244 Tausend Euro jährlich zuzüglich Besoldungserhöhungen. Nicht zuletzt durch diese Maßnahme wird dem „Nationalen Programm Deutschlands zur Durchführung der Verordnung (EG) 725/2004 des Europäischen Parlaments und des Rates vom 31.03.2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen“ Rechnung getragen. In diesem wird unter „Operatives Management zur Gefahrenabwehr“ benannt, dass zur effizienten und kompetenten Durchführung der hafensicherheitsbehördlichen Aufgaben Kompetenzen sowohl im Bereich „Öffentliche Sicherheit“ als auch „Häfen“ erforderlich sind. Durch diese Kompetenzbündelung aus den zwei Bereichen wird eine kompetente und effiziente Aufgabenerfüllung sichergestellt.

6. Welche Mittel sind gemäß Haushalt 2025 gegebenenfalls für die Stärkung der kritischen Infrastruktur vorgesehen?

Zur Beantwortung dieser Frage werden zunächst alle Mittel zur Stärkung der digitalen Resilienz im Sektor Staat und Verwaltung aufgeführt, ohne dabei zu unterscheiden, ob es sich dabei um Kritische Infrastrukturen handelt oder nicht (siehe auch die Vorbemerkung der Landesregierung und die Beantwortung der Fragen 1 und 5). Investitionen zur Stärkung der Resilienz für die Themen BCM und Cybersicherheit, analog zur Beantwortung der Frage 5, stellen sich wie folgt dar:

Jahr	Bereich	Art	Finanzielle Mittel
2025	Staat und Verwaltung Kommunen	Unterstützung beim BCM	133.732,00 Euro
2025	Staat und Verwaltung Landesverwaltung	Unterstützung beim BCM	82.107,45 Euro

Das MWK hat vom MI für das Jahr 2025 insgesamt Haushaltsmittel in Höhe von 177 600 Euro für Maßnahmen im Rahmen der Implementierung und des Aufbaus eines Business Continuity Management Systems (BCMS) erhalten, darunter 28 000 Euro zur Einrichtung der ressorteigenen Stabsräume, 7 500 Euro zur Ausbildung des Notfall- und Krisenstabs und 142 100 Euro für die externe Unterstützung für befristete Aufgaben. Zudem sind 50 000 Euro für die satellitengestützte Kommunikation geplant, die MI zentral fördert.

Im Katastrophenschutz sind in 2025 planmäßig 250 000 Euro für die Stärkung der Kritischen Infrastruktur vorgesehen.

7. Plant die Landesregierung gegebenenfalls, für potenzielle Bedrohungen (Naturkatastrophen, Cyberangriffe, Sabotageakte, physische Angriffe etc.) jeweils spezifische Lösungsstrategien zu entwickeln? Wenn ja, wie sollen diese Strategien ausgestaltet sein, und in welcher Form sollen dabei externe Akteure wie beispielsweise zivilgesellschaftliche Organisationen, wissenschaftliche Einrichtungen oder privatwirtschaftliche Partner einbezogen werden?

Die physischen Auswirkungen derartiger Bedrohungen unterscheiden sich wenig von ähnlich gelagerten herkömmlichen Schadensereignissen und werden im Rahmen des All-Gefahren-Ansatzes von der Gefahrenabwehr mit bewährten Strategien und Mitteln bewältigt.

Angesichts der Komplexität der Auswirkungen der veränderten Sicherheitslage auf den Zivil- und Katastrophenschutz in Niedersachsen ist es erforderlich, im Rahmen einer ganzheitlichen Betrachtung die wesentlichen Ziele und abgeleiteten Handlungserfordernisse zur zielgerichteten Fortentwicklung des Katastrophenschutzes herauszuarbeiten.

Im MI wird daher zurzeit eine Strategie Katastrophenschutz Niedersachsen, die die Ausrichtung des Katastrophenschutzes für die kommenden Jahre und die vorrangigen Handlungsfelder darstellen wird, erarbeitet. Eines der bedeutsamen Handlungsfelder ist dabei die Stärkung der Resilienz, beispielsweise durch die Etablierung von Krisenmanagementstrukturen auf allen behördlichen Ebenen, die wirksame Absicherung Kritischer Infrastrukturen sowie die Sensibilisierung der Bevölkerung und die Steigerung ihrer Selbsthilfefähigkeit.

Die gesundheitliche Versorgung der Zivilbevölkerung ist Aufgabe der Länder. In Friedenszeiten ist eine medizinische Erstversorgung bei Großschadenslagen und Katastrophen gewährleistet. Die Länder haben jedoch ergänzende Maßnahmen zur gesundheitlichen Versorgung im Verteidigungsfall zu planen.

Für den Bereich des medizinischen Zivil- und Bevölkerungsschutzes gab es bisher keine rechtliche Grundlage eines Sicherstellungsgesetzes. Es bedarf hier somit einer Notfall- und Vorsorgeplanung, um eine adäquate Reaktionsfähigkeit des Gesundheitswesens auf zivile und militärische Zwischenfälle außerhalb des Regelbetriebs sicherzustellen. Dazu erarbeitet der Bund seit dem Frühjahr gemeinsam mit den Ländern in Bund-Länder offenen Arbeitsgruppen (BLoAG) die Grundlagen für das

neue Gesundheitssicherstellungsgesetz. Dabei werden auch die entsprechenden Verbände in die jeweiligen BLoAGs eingebunden.

Ziel ist es dabei, dass die BLoAG anhand von Szenarien unterschiedlichste Bedrohungslagen, Versorgungsausfälle und weitere Krisenszenarien erarbeiten. Dabei sollen die notwendigen gesetzlichen Neuregelungen sowie notwendige Ergänzungen an bereits bestehenden rechtlichen Regelungen ermittelt und im neuen Gesundheitssicherstellungsgesetz zusammengefasst werden.

8. Inkludiert die Cybersicherheitsstrategie[2] Niedersachsens gegebenenfalls spezifische Maßnahmen, um die niedersächsische kritische Infrastruktur gegen Cyberangriffe zu schützen? Wenn ja, welche?

Der Landesregierung ist bewusst, dass die kritische Infrastruktur zunehmenden Cyberbedrohungen ausgesetzt ist und damit das Gemeinwohl immer stärker von der Resilienz digitaler Infrastrukturen abhängig ist. Damit hat der Schutz kritischer Infrastruktur gegen Cyberbedrohungen hohe strategische Bedeutung. Die Landesregierung hat deshalb mit der Cybersicherheitsstrategie Niedersachsen den Beschluss gefasst, Unternehmen, die von regulatorischen Vorgaben betroffen sind sowie Einrichtungen, die ihre Aufgabe der (regionalen) Daseinsvorsorge unterhalb regulatorischer Schwellenwerte wahrnehmen, bei der Umsetzung von Cybersicherheitsmindestanforderungen zu unterstützen.

Im Zuge des Inkrafttretens der NIS-2-Richtlinie hat das damalige Ministerium für Inneres und Sport mit dem damaligen Ministerium für Wirtschaft, Verkehr, Bauen und Digitalisierung ein Informationsangebot für erstmalig regulierte Unternehmen bereitgestellt.

Das MI veranstaltet regelmäßige KRITIS-Tagungen für Unternehmen und Cybersicherheitstage für die Landes- und Kommunalverwaltung, um über neue regulatorische Vorgaben zu informieren, vor aktuellen Gefährdungen zu warnen und gemeinsam mit den Teilnehmenden in den Austausch zu gehen.

Insbesondere der Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes als auch die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Niedersachsen stehen den kritischen Infrastrukturen als auch den erstmalig durch die NIS-2-Richtlinie regulierten Unternehmen mit ihrem Informations- und Unterstützungsangebot zur Verfügung.

Ein weiterer Ausbau der gesamtstaatlichen Cybersicherheitsarchitektur - einschließlich spezifischer Maßnahmen - findet kontinuierlich statt. Hierbei haben die Konsolidierung sowie die zentrale Koordinierung und Steuerung durch das übergreifende Cybersicherheitsmanagement im MI besondere Bedeutung. Die Konzeption für eine bedarfsgerechte Weiterentwicklung des übergreifenden Cybersicherheitsmanagements zu einem Koordinierungs- und Steuerungszentrum im Bereich digitaler Resilienz, wie im Koalitionsvertrag der regierungstragenden Parteien vorgesehen, wird aktuell an veränderte Rahmenbedingungen, etwa auf Bundesebene, angepasst.

[2] https://www.stk.niedersachsen.de/startseite/presseinformationen/landesregierung-beschliesst-neue-cybersicherheitsstrategie-235834.html