Stellungnahme zum Fragenkatalog „KRITIS“ der Enquetekommission „Krisen- und Notfallmanagement“ (EK II – KRITIS – 01.03.2024)

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/1295

A41

1. Grundlagen

1.1 Welche staatlichen und privatwirtschaftlichen Einrichtungen werden als kritische Infrastruktur betrachtet und warum?

Die Bundesressorts haben sich auf die folgende **qualitative Definition** kritischer Infrastrukturen geeinigt: „Kritische Infrastrukturen (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“ [1].

In einem ersten Schritt wurden auf Bundesebene acht, auf Bund-Länder-Ebene neun **Sektoren** definiert, die wiederum durch Branchen konkretisiert werden können. Unternehmen und Organisationen, die unter diese Definitionen fallen, können sowohl privatwirtschaftlicher, als auch staatlicher Natur sein. Tabelle 1 zeigt die Sektoren nach sie definierender Stelle. Durch die unterschiedlichen Betrachtungsweisen können insgesamt 10 Sektoren identifiziert werden.

Tabelle 1: Sektoren kritischer Infrastrukturen nach definierender Stelle

Sektor	KRITIS nach Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)	KRITIS nach Beschluss durch Bund-Länder-AG
Energie	x	x
Wasser	x	x
Ernährung	x	x
Informations- und Kommunikationstechnik	x	x
Finanz- und Versicherungswesen	x	x
Transport und Verkehr	x	x
Gesundheit	x	x
Siedlungsabfallentsorgung	x (nachträglich)	
Staat und Verwaltung		x
Medien und Kultur		x

Die (IT-)Sicherheit kritischer Infrastrukturen in Deutschland wird durch das BSI-Gesetz (BSIG, BSI = Bundesamt für Sicherheit in der Informationstechnik) und die BSI-Kritisverordnung (BSI-KritisV) geregelt. Diese definieren, welche Bereiche als kritisch gelten und welche **Schwellenwerte, also quantitative Kriterien,** für Betreiber gelten, um als kritisch eingestuft zu werden. Das erste IT-Sicherheitsgesetz von 2015 und das zweite IT-Sicherheitsgesetz von 2021 haben das BSI-Gesetz erweitert und dem BSI neue Kompetenzen verliehen, um die Cybersicherheit zu stärken.

Zum einen fehlen hier jedoch (s. Tabelle 1, Spalte 2) Behörden als Kritische Infrastrukturen (Sektor Staat und Verwaltung) sowie der Sektor Kultur und Medien und damit u.a. auch die Warnung der Bevölkerung [2].

Dr.-Ing. Sylvia Bach, Bergische Universität Wuppertal, Fachgebiet Bevölkerungsschutz, Katastrophenhilfe und Objektsicherheit

Zum anderen ist die betrachtete Ebene der Bund. Die quantitativen Kriterien (u. a. 500.000 versorgte Personen) sind dementsprechend oft nicht auf die Landes- und kommunale Ebene übertragbar.

Auf Bundesebene können Unternehmen also mit Hilfe der Anwendung qualitativer und quantitativer Kriterien, die im BSIG bzw. der BSI-KritisV verankert sind, eindeutig feststellen, ob sie den kritischen Infrastrukturen zuzuordnen sind oder nicht.

Auf der Landesebene oder im kommunalen Kontext muss das Identifizierungsverfahren angepasst werden, „etwa indem eine Teilmenge der Sektoren ausgewählt oder Dienstleistungen ergänzt werden (qualitatives Kriterium) oder indem die Höhe der Schwellenwerte justiert wird (quantitatives Kriterium)“ [3]. Eine Identifizierungshilfe gibt die Broschüre des Bundesamtes für Bevölkerungsschutz, Katastrophenhilfe und Objektsicherheit „Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten“ [2].

Die **Einstufung** als kritische Infrastruktur im nationalen Recht erfolgt in grob vereinfachter Form in drei Stufen: Zunächst muss eine kritische Dienstleistung in einem der acht kritischen Sektoren gemäß § 2 BSIG erbracht werden. Diese Dienstleistung erfordert den Betrieb einer Anlage, die einer bestimmten Kategorie gemäß der BSI-KritisV zugeordnet ist. Darüber hinaus wird der Versorgungsgrad der Dienstleistung als bedeutend angesehen, wenn die entsprechenden Schwellenwerte überschritten werden, üblicherweise 500.000 versorgte Personen [4].

1.2 Welche Einrichtungen sind konkret im Kontext von Pandemien und Extremwetterereignissen betroffen?

Ein wichtiges, in der Vorbereitung auf jegliche Krisen häufig unterschätztes Problem ist die Eigenbetroffenheit von Mitarbeiter*innen. Dies trifft auf Organisationen im Katastrophenschutz, wie z. B. die Feuerwehr, Hilfsorganisationen, das THW etc. genauso zu, wie auf Unternehmen der Energieversorgung, des Gesundheitswesens, der Abfallentsorgung, des Transportwesens etc., also kritischen Infrastrukturen nach BSIG. In einer Pandemie ist dies eine besonders hervorzuhebende Herausforderung, da überörtliche Hilfe aufgrund der flächendeckenden Problematik oftmals nicht möglich ist.

<u>Pandemie</u>

Die Eindämmungsmaßnahmen im Zuge des Pandemiemanagements können ebenso die Betriebsfähigkeit beeinträchtigen, wie die Pandemie selber, da sie zu Schließungen, Reisebeschränkungen und anderen Einschränkungen führen können. Die Schließung von Kindergärten und Schulen z. B., die bisher formal nicht als KRITIS gelten, steigert das eingangs beschriebene Problem der Eigenbetroffenheit, da neben erkrankten Mitarbeiter*innen auch solche zu Hause bleiben müssen, die die Betreuung ihrer Kinder sicherstellen müssen. Im Folgenden werden Beispiele betroffener kritischer Infrastrukturen genannt und der Zusammenhang zu einem Pandemiegeschehen hergestellt.

Gesundheitseinrichtungen: Krankenhäuser, Arztpraxen, Apotheken und andere medizinische Versorgungszentren sind als Hauptanlaufstellen für die Behandlung von infizierten Personen besonders betroffen. Sie müssen ihre Kapazitäten erhöhen, um die steigende Anzahl von Patient*innen zu bewältigen, und benötigen neben ausreichender Schutzausrüstung und Medikamenten dementsprechend auch ausreichend Personal.

Ernährungsinfrastruktur: Lebensmittelgeschäfte, Lebensmittelproduktionsstätten und Logistikunternehmen sind entscheidend, um die kontinuierliche Versorgung mit Lebensmitteln

Dr.-Ing. Sylvia Bach, Bergische Universität Wuppertal, Fachgebiet Bevölkerungsschutz, Katastrophenhilfe und Objektsicherheit

sicherzustellen. Engpässe können auftreten, wenn Mitarbeiter*innen erkranken oder Lieferketten unterbrochen werden.

Telekommunikations- und Informationsinfrastruktur: Mit der Zunahme von Home Office und Home Schooling während einer Pandemie steigt die Nutzung von Internet- und Kommunikationsdiensten stark an. Die Stabilität und Sicherheit dieser Infrastruktur sind dementsprechend von besonderer Bedeutung, nicht zuletzt, um sicherstellen zu können, dass wichtige Informationen die Bevölkerung erreichen. Demgegenüber steht ein erhöhtes Risiko von Cyberangriffen, einerseits, weil eine erhöhte Nutzung auch eine größere mögliche Angriffsfläche bietet und andererseits, weil Unternehmen eventuell unter Zeitdruck digitale Lösungen entwerfen, deren Sicherheit nicht ausreichend getestet werden kann.

Energieversorgung: Die Energieinfrastruktur muss stabil bleiben, um sicherzustellen, dass Krankenhäuser, Lebensmittelgeschäfte und andere kritische Einrichtungen weiterhin mit Energie versorgt werden können.

Transport und Verkehr: Öffentliche Verkehrsmittel und Logistikunternehmen spielen eine wichtige Rolle bei der Bereitstellung von lebenswichtigen Gütern und der Mobilität von Personen, insbesondere für medizinisches Personal und andere Schlüsselkräfte.

<u>Extremwetterereignisse</u>

Neben der Problematik der eingangs beschriebenen Eigenbetroffenheit, die zu Personalmangel auch in kritischen Infrastrukturen führen kann, sind im Falle von Extremwetterereignissen vor allem physische Infrastrukturen betroffen. Im Folgenden werden Beispiele potentiell betroffener Anlagen aufgeführt.

Energieinfrastruktur: Kraftwerke, Stromleitungen und Umspannwerke sind anfällig für Schäden durch Stürme, Überschwemmungen, Blitzeinschläge oder extreme Hitze. Diese Ereignisse können zu Stromausfällen führen, die die Versorgung von Haushalten, Unternehmen und wiederum anderen kritischen Einrichtungen beeinträchtigen.

Wasserinfrastruktur: Wasserwerke, Kläranlagen und Wasserversorgungssysteme können durch Überschwemmungen, Starkregen oder Stürme beschädigt werden. Dies kann zu Unterbrechungen der Wasserversorgung, Verunreinigungen des Trinkwassers und sanitären Problemen führen.

Transportinfrastruktur: Straßen, Brücken, Schienenwege und Flughäfen können durch Extremwetterereignisse beschädigt oder unpassierbar gemacht werden. Dies kann den Güterverkehr einschränken, die Mobilität von Personen behindern und zur Unterbrechung von Lieferketten führen.

Kommunikationsinfrastruktur: Telekommunikationsmasten, Kabelnetze und Satellitenverbindungen können durch Stürme, Blitzeinschläge oder Überschwemmungen beschädigt werden. Dies kann zu Ausfällen von Telefon-, Internet- und Mobilfunkdiensten führen, was die Kommunikation und den Informationsaustausch beeinträchtigt.

Gesundheitsinfrastruktur: Krankenhäuser, medizinische Einrichtungen und Notfalldienste können durch Extremwetterereignisse beschädigt und beeinträchtigt werden, was zu Unterbrechungen bei der Patientenversorgung oder dem Ausfall lebenswichtiger medizinischer Geräte führen kann.

Weitere Einschränkungen (bezogen auf beide Szenarien) sind überall dort zu erwarten, wo Schäden und Unterbrechungen aufgrund von Abhängigkeiten von Strom, Wasser, Transport und Kommunikation möglich sind, z. B. im Ernährungssektor. Extremwetterereignisse können auch zu

erhöhten Betriebs- und Reparaturkosten durch Wiederaufbaumaßnahmen sowie zu erhöhten Versicherungskosten führen, was die (finanzielle) Widerstandsfähigkeit der betroffenen Einrichtungen beeinträchtigen kann.

1.3 Welche gesetzlichen Regelungen ergeben sich aus der Zuordnung zur kritischen Infrastruktur? Wie sind diese in die föderalistischen Strukturen einzuordnen?

a) Identifikation und Registrierung

Unternehmen sind dafür verantwortlich, ihre Dienstleistungen und/oder Anlagen zu identifizieren, die nach BSIG bzw. BSI-KritisV den kritischen Infrastrukturen zuzuordnen sind. Diese müssen dann eigenverantwortlich dem BSI gemeldet und dort registriert werden, außerdem muss eine Kontaktstelle eingerichtet und dem BSI benannt werden.

b) Ergreifung geeigneter Maßnahmen, inkl. Sicherheit in der Informationstechnik und Angriffs-erkennung

Nach §8a BSIG sind Unternehmen, die kritische Anlagen und/oder Dienstleistungen betreiben bzw. anbieten dazu 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“ [5]. Dies muss zügig erfolgen, genauer spätestens am ersten Werktag nach der unter a) beschriebenen Identifikation. Dies umfasst seit dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Hierfür sollen „geeignete Paramater“ kontinuierlich erfasst werden und zu einer automatischen Erkennung von Bedrohungen beitragen.

c) Informations- und Meldepflicht

Nach §8b BSIG muss der Betreiber Störungen an das BSI melden.

d) Nachweispflicht

Nach §8a BSIG müssen Betreiber die unter b) genannten Maßnahmen regelmäßig nachweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Einige dieser Pflichten werden sich ggfs. durch die Umsetzung der europäischen NIS2-Richtlinie [6] und das kommende KRITIS-Dachgesetz [7] (nationale Umsetzung der europäischen Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) [8]) verändern, vor allem, aber nicht ausschließlich, bezüglich der Meldewege. Auch zusätzliche Pflichten sind möglich.

Wie bereits unter 1.1 erläutert, ist der Geltungsbereich des BSIG vor allem für große, bundesweit agierende Organisationen von Belang. Zwar muss jedes Unternehmen seine Anlagen und Dienstleistungen auf Kritikalität nach BSIG untersuchen, ein Unterschreiten der Schwellenwerte bedeutet allerdings nicht zwangsläufig, dass die untersuchten Anlagen und Dienstleistungen nicht kritisch in Bezug auf die zu versorgende Bevölkerung wären. Nach bisheriger Kenntnis der Autorin zieht eine nach angepassten Schwellenwerten (siehe Leitfaden [2]) identifizierte Anlage oder Dienstleistung jedoch keine Betreiberpflichten nach sich.

1.4 Gibt es aus Ihrer Sicht weitere Einrichtungen, die der kritischen Infrastruktur zuzuordnen sein könnten? Wenn ja, warum?

Für die Erhöhung der gesellschaftlichen Resilienz kann es von Vorteil sein, weitere Einrichtungen oder sogar Sektoren/Branchen der kritischen Infrastruktur zuzuordnen.

Wie unter 1.1 und 1.3 erläutert, greifen die vorhandenen Gesetze und damit einhergehende Verpflichtungen für Betreiber nur für acht der insgesamt 10 in Deutschland definierten KRITIS-Sektoren. Und hier auch nur, wenn die erwähnten Schwellenwerte erreicht werden.

Dementsprechend könnte es sinnvoll sein, bundeslandspezifische Schwellenwerte/Kriterien festzulegen. Dies würde zu einer noch **gezielteren Identifikation kritischer Infrastrukturen in NRW** führen. Im Moment existieren jedoch – nach Kenntnis der Autorin – nicht die für eine solche Evaluation notwendigen Strukturen, d.h. Meldewege und entsprechende aufsichtführende Behörden. Das noch in diesem Jahr in Kraft tretende KRITIS-Dachgesetz wird voraussichtlich solche Meldewege auch auf Länderebene vorsehen. Die Ausweitung der Pflichten aus dem BSIG auf weitere (ggfs. kleinere) Unternehmen kann des Weiteren zu unverhältnismäßigem organisatorischen und administrativen Aufwand in den betroffenen Organisationen führen.

Die gleiche Problematik beträfe die Aufnahme weiterer Sektoren oder Branchen in den Kreis der kritischen Infrastrukturen, auch wenn eine kontinuierliche Erfassung und der damit einhergehende besondere Schutz durchaus zur Verbesserung der gesamtgesellschaftlichen Resilienz beitragen können.

Dies gilt zum Beispiel für Bildungseinrichtungen, und hier insbesondere für **Kindergärten und Schulen**. Ihnen einen besonderen Status zukommen zu lassen, um der unter 1.2 genannten Eigenbetroffenheit besser entgegenwirken zu können, kann im Krisenfall – wie während der Pandemie in NRW gesehen – einen entscheidenden Unterschied machen.

Eine weitere Branche, deren Kritikalität unter Umständen gegeben sein könnte, ohne dass dies nach nationalen Vorgaben der Fall ist, sind **Forschungseinrichtungen**, die kritische Forschungs- und Entwicklungsdienste erbringen. Beispiele wären u.a. pharmazeutische Forschungseinrichtungen oder solche zur IT- und Cybersicherheitsforschung.

1.5 Gibt es unterschiedlicher Einstufungen für unterschiedliche Szenarien?

Der Kenntnis der Autorin nach ist dies nicht der Fall. Kritikalität wird in Deutschland szenarienunabhängig nach den unter 1.1 beschriebenen Kriterien definiert.

1.6 Hat sich diese Einordnung in der Pandemie bewährt?

Falls hiermit die Einordnung kritischer Infrastrukturen in die o.g. Sektoren gemeint ist: nach Einschätzung der Autorin hat sich diese in der Pandemie weitestgehend bewährt. Die vom Ministerium für Arbeit und Gesundheit NRW im März 2020 erlassene **Leitlinie zur Bestimmung des Personals kritischer Infrastrukturen** zielte darauf ab, den im Lockdown nicht zulässigen Kindergarten- und Schulbesuch für Kinder zu ermöglichen, deren Eltern bestimmten, systemrelevanten Tätigkeiten nachgingen. Diese Berufe sind in der Leitlinie spezifiziert und inkludieren neben Angehörigen „klassischer“ kritischer Infrastrukturen auch solche von Hochschulen und sonstigen wissenschaftlichen Einrichtungen, „soweit sie für den Betrieb von sicherheitsrelevanten Einrichtungen oder unverzichtbaren Aufgaben zuständig sind“ [9] und - konsequenterweise - des Sektors „Schulen, Kinder- und Jugendhilfe, Behindertenhilfe“. Dies zeigt nach Ansicht der Autorin, dass einer Pandemie

angemessene Maßnahmen ergriffen werden konnten, um kritische Infrastrukturen im Sinne der vorliegenden Krise zu schützen; zumindest bezüglich eventueller Personalengpässe durch den Mangel an Kinderbetreuungsmöglichkeiten.

1.7 Welche konkreten Zuständigkeiten und Aufgaben werden den Akteuren im Rahmen der föderalistischen Strukturen zuteil?

Kritische Infrastrukturen und deren Anlagen unterliegen durch ihre geographische Lage einer **kommunalen Aufsicht**. Sie erstrecken sich jedoch häufig über kommunale Grenzen hinweg und vor allem haben Ausfälle Auswirkungen über diese Grenzen hinweg. Durch ihre Einordnung als kritische Infrastruktur unterliegen sie zudem der **Aufsicht des BSI**. Um diesem Zuständigkeitsproblem, bzw. dem daraus potentiell entstehenden Koordinierungsproblem entgegenzuwirken, gibt es verschiedene Maßnahmen und Kooperationen zwischen den Akteur*innen.

Die **Bund-Länder Arbeitsgruppe für den Schutz kritischer Infrastrukturen** (AG KOST KRITIS) existiert seit 2012 und bietet eine Austauschplattform zwischen Behörden auf Landes- und Bundesebene. Ziel ist es, das gemeinsame Verständnis hinsichtlich der Aufgaben beim Schutz kritischer Infrastrukturen zu stärken und Kompetenzen zu bündeln. In ihr wirken Mitarbeiter*innen des Bundesministeriums des Innern (BMI) sowie Vertreter*innen aller Bundesländer mit.

„**UP KRITIS**" ist eine öffentlich-private Partnerschaft zum Schutz kritischer Infrastrukturen und dient der Verbesserung der Zusammenarbeit von Betreibern kritischer Infrastrukturen und staatlichen Organisationen. Die Geschäftsstelle befindet sich im BSI, dort kann sich jedes Unternehmen sowie behördliche Stellen für eine Teilnahme am UP KRITIS anmelden. Das BSI stellt neueste Erkenntnisse zur Cybersicherheit zur Verfügung und in Themen- und Branchenarbeitskreisen werden strategisch-konzeptionelle Fragestellungen bearbeitet. So kann ein fachlicher Austausch stattfinden, der durch einen Stab und die Geschäftsstelle unterstützt wird.

1.8 Welche Auswirkungen sind durch Funktionseinschränkungen im Bereich KRITIS zu erwarten?

Diese Frage ist nicht pauschal beantwortbar. Eine sehr gute Zusammenfassung und Aufstellung der Abhängigkeiten kritischer Infrastrukturen untereinander sowie die Abhängigkeiten der Gesellschaft bietet der Bericht des Büros für Technikfolgenabschätzung im Deutschen Bundestag (TAB) „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“ von 2010 [10].

Kaskadeneffekte und Interdependenzen im Bereich kritischer Infrastrukturen können besonders anschaulich am Beispielszenario Stromausfall aufgezeigt werden, da fast unser gesamtes Privat- und Arbeitsleben auf eine funktionierende Stromversorgung angewiesen ist.

Allgemeine Auswirkungen von Funktionseinschränkungen bei kritischen Infrastrukturen können neben den zu erwartenden Störungen der Versorgungssicherheit im Ernährungs- oder Gesundheitssektor auch wirtschaftliche Auswirkungen durch Produktionsausfälle oder Lieferkettenunterbrechungen sein. Bei Ausbleiben der Befriedigung grundlegender Bedürfnisse wie Wasser, Nahrung oder gesundheitliche Versorgung muss mit einem höheren Risiko von gesellschaftlichen Unruhen gerechnet werden. Die These/Annahme, dass es im Katastrophenkontext zu egoistischem und kriminellem Verhalten kommt, ist jedoch wissenschaftlich nicht bewiesen und eher umstritten [11]. Demgegenüber ist nachgewiesen, dass Angst, Stress und psychische Belastungen vor allem bei jungen Menschen langfristige Auswirkungen auch nach dem Überstehen der Krise haben können. [12].

1.9 Wie wirken sich diese Funktionseinschränkungen konkret im Falle des Auftretens von Pandemien und/oder Extremwetterereignissen aus?

Bei Extremwetterereignissen ist es häufig zunächst die physische Betroffenheit von Anlagen und Betriebsstätten und die daraus resultierenden Funktionseinschränkungen, die dazu führen, dass auch die nicht direkt betroffene Bevölkerung Auswirkungen bemerkt.

Im Falle der Hochwasserkatastrophe in NRW und Rheinland-Pfalz im Juli 2021 waren z.B. in großem Umfang Netzstationen, Umspannanlagen und Leitungen von der Flut betroffen, was zu Unterbrechungen in der Stromversorgung nicht nur von Haushalten führte, die mit den direkten Auswirkungen des Hochwassers zu kämpfen hatten. Hitze- und Dürreperioden können ein weiteres Beispiel für solche direkten und indirekten Auswirkungen sein; neben den gesundheitlichen Gefahren vor allem für Babys, Kleinkinder und ältere sowie chronisch erkrankte Menschen [12b, 12c] hat das mit Dürreperioden verbundene Niedrigwasser in Flüssen einen negativen Einfluss auf die Binnenschifffahrt, was bereits 2018, 2020 und 2023 zu wirtschaftlichen Einbußen führte [12d] und in der Folge auch Versorgungseinschränkungen verursachen kann.

Die Auswirkungen von Pandemien (und Epidemien) auf kritische Infrastrukturen werden in Teilen 2011 im BMI-Leitfaden zum Risiko- und Krisenmanagement für Unternehmen und Behörden beschrieben [14] sowie in den Berichten zur Risikoanalyse im Bevölkerungsschutz von 2013 und 2023 [12e, 12f] und dem Auswertungsbericht zur länderübergreifenden Krisenmanagementübung (LÜKEX) 2007 [12g]. Durch die bereits erwähnte Eigenbetroffenheit (neben einer Erkrankung schließt dies auch die Pflege von erkrankten Angehörigen ein) können sowohl kritische Produktionsstätten als auch kritische Dienstleistungen von Personalmangel betroffen sein, der neben wirtschaftlichen Einbußen auch zu Einschränkungen bzgl. der angebotenen kritischen Produkte oder Dienstleistungen führen kann. Eine enge Verzahnung von Lieferketten und gegenseitige Abhängigkeiten können wiederum zu „Dominoeffekten“ führen [14]. Der LÜKEX-Auswertungsbericht führt tabellarisch Empfehlungen auf, die sich aus der Übung 2007 ableiten lassen. Hier sind u.a. „Regelungen zur Sicherstellung der personellen Besetzung für Schlüsselbereiche kritischer Infrastrukturen, (z.B. Störfallbetriebe, Kernkraftwerke, ambulante und stationäre medizinischer Versorgung und Pflege)“ sowie eine „verstärkte Einbindung der privaten Betreiber kritischer Infrastrukturen in das Netzwerk für bereichsübergreifendes Krisenmanagement“ genannt [12g]. Auch der Bericht zur Risikoanalyse 2012 gibt Empfehlungen, wie sich Behörden auf pandemische Ereignisse vorbereiten können und zeigt zudem auf, welche Auswirkungen solche Ereignisse auf kritische Infrastrukturen haben können. Die zeitnahe Einberufung von Krisenstäben gehört ebenso dazu wie klare Kommunikation mit abgestimmten Begriffen [12e]. Nicht eindeutige Kommunikation von Akteur*innen untereinander (z.B. zwischen Krankenhäusern und Gesundheitsämtern oder Gesundheitsämtern und unteren Katastrophenschutzbehörden) kann ebenso zu Missinterpretationen und Missverständnissen führen, wie die uneindeutige oder mangelhaft erläuternde Kommunikation von Statusberichten, Maßnahmen und Empfehlungen der Behörden in die Bevölkerung. Die in weiten Teilen fehlende Umsetzung von Empfehlungen aus beiden Berichten [12g und 12e] wird im „Bericht zur Risikoanalyse im Bevölkerungsschutz 2020 bis 2022“ bemängelt, die Coronapandemie habe „deutlich gemacht, welchen Nutzen diese fachlich fundierte Arbeit *hätte entfalten können*“ [12f].

Die weitreichenden Auswirkungen sowohl von Pandemien als auch von Extremwetterereignissen auf kritische Infrastrukturen in Deutschland sind also in großen Teilen bekannt, wurden in entsprechenden

Risikoanalysen untersucht und es wurden konkrete Handlungsempfehlungen abgeleitet und veröffentlicht.

1.10 Welche Bedeutung haben aus Ihrer Sicht Bildungs-, Betreuungs- und Erziehungseinrichtungen im Hinblick auf Kritikalität und Vulnerabilität der Infrastrukturen?

Wie in 1.4 und 1.6 erläutert, haben die genannten Einrichtungen eine zentrale Bedeutung im Hinblick auf die Vulnerabilität kritischer Infrastrukturen. Diese Bedeutung hervorzuheben und Einrichtungen dieser Art resilienter gegen Krisen zu machen, birgt das Potential, das Problem der Eigenbetroffenheit von Berufsgruppen in kritischen Infrastrukturen zu mindern.

2. KRITIS

2.1 Wodurch werden die kritischen Infrastrukturen im Fall einer Krise in einen Krisenmodus versetzt und was bewirkt das im Einzelnen?

Wie in 1.3, Absatz b) beschrieben, haben Betreiber kritischer Infrastrukturen nach dem BSIG die Pflicht, unter anderem auch „angemessene *organisatorische* […] Vorkehrungen“ zu treffen um die Funktionsfähigkeit der von ihnen betriebenen Anlagen zu sichern. Solche organisatorischen Maßnahmen sind sinnvollerweise in einem organisatorischen Risiko- und Krisenmanagement institutionalisiert. Aus der von der Bundesregierung 2009 beschlossenen „Nationalen Strategie zum Schutz kritischer Infrastrukturen“ [13] ging ein Leitfaden zum Risiko- und Krisenmanagement für Unternehmen und Behörden hervor [14], der den Aufbau und die Pflege solcher Systeme beschreibt.

Ein wichtiger Aspekt dieses organisatorischen Krisenmanagements ist die Etablierung eines **Krisenstabes** (auch: Besondere Aufbauorganisation, BAO, genannt) inkl. der Benennung und Schulung seiner Mitglieder, der Festlegung von Zuständigkeiten, Verantwortlichkeiten, entsprechender Melde- und Alarmierungswege sowie einer Maßnahmenplanung. Diese Vorplanung findet im Normalbetrieb statt. Im Falle einer Krise wird der verantwortliche Krisenmanager/die verantwortliche Krisenmanagerin, der Vorstand oder eine andere geeignete Person diesen Krisenstab einberufen. Wann dies geschieht, hängt im Einzelfall von der Qualität der vorhandenen Informationen, aber auch von der persönlichen Erfahrung der beteiligten Personen sowie ggfs. vorab festgelegten individuellen Schwellenwerten ab.

Behördliche und unternehmerische Krisenstäbe können sich dabei stark voneinander unterscheiden. Während behördliche Stäbe in operativ-taktische Einsatzleitungen sowie administrativ-organisatorische Verwaltungsstäbe eingeteilt werden können, von denen erstere immer und letztere fast immer nach Feuerwehr-Dienstvorschrift 100 organisiert sind [14b], unterliegen unternehmerische Stäbe - und damit auch solche im Krisenmanagement des Großteils der kritischen Infrastrukturen angesiedelte - nicht dieser Vereinheitlichung.

Ist der Krisenstab einberufen, ist die Grundlage dafür geschaffen, die in einer Krise u.U. notwendigen zeitkritischen und ggfs. ungewöhnlichen Entscheidungen zu treffen. Der Krisenstab ist dann die BAO, „die die normale Aufbauorganisation zur Bewältigung von besonderen Lagen für die beteiligten Organisationseinheiten durchbricht und abteilungsübergreifend Kompetenzen unter einer einheitlichen Leitung bündelt. Beim Krisenstab handelt es sich um ein **Entscheidungsinstrument** mit koordinierenden, informierenden, beratenden und unterstützenden Zusatzfunktionen. Formal besteht der Krisenstab aus einem Leiter und dem Krisenstabsteam“ [14].

Die theoretische Wirksamkeit und Sinnhaftigkeit eines Krisenstabes sind unumstritten. Wie effektiv ein unternehmerischer oder behördlicher Krisenstab agieren kann, hängt jedoch von verschiedenen Faktoren ab. Bereits oben genannt sind **Zuständigkeiten und Meldewege**: beide müssen klar definiert sein, um effizientes Arbeiten zu ermöglichen. Dies muss zwingend im Vorfeld einer Krise geschehen, da die Festlegung solcher Kriterien unter Zeitdruck fehleranfällig ist. Die **Qualifikation und Erfahrung** der Mitglieder im Stab sind weitere wichtige Kriterien. Je erfahrener und/oder besser ausgebildet diese sind, desto effektiver können sie die anstehenden, meist komplexen Aufgaben erledigen, sich an veränderte Umstände anpassen und relevante von weniger relevanten Informationen unterscheiden. Ausbildung und Qualifikation sind also essentiell in der Vorbereitung. Allgemein benötigt ein Krisenstab Zugang zu den für die Bewältigung der Krise notwendigen **Ressourcen** (z.B. Personal, Material, Finanzmittel), die **Rückendeckung der Unternehmens- oder Behördenführung** ist dementsprechend ein weiterer kritischer Aspekt, der sich auch auf die Umsetzung der getroffenen Entscheidungen auswirken kann.

Laut dem „Bericht zur Hochwasserkatastrophe 2021“ sind auf Anfrage der Innenministerkonferenz (IMK) die Schulungskapazitäten für behördliche und unternehmerische Krisenstäbe (administrativ-organisatorische Stäbe) der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) erweitert, sowie das Angebot quantitativ erhöht worden [15].

2.2 Gibt es konkrete Schwellenwerte, die überschritten werden müssen, damit der Krisenmodus ausgerufen wird? Sind diese gesetzlich festgelegt? Falls nein, sollten aus Ihrer Sicht Schwellenwerte definiert und festgelegt werden? Wie könnte dies geschehen?

Nach Kenntnis der Autorin gibt es keine solchen gesetzlich festgelegten **Schwellenwerte**. Die unter 1.9 beschriebene Notwendigkeit klar definierter Begrifflichkeiten ist eine der Schwierigkeiten, die hier zutage treten. Ob z.B. eine Kommune, eine Behörde oder ein Unternehmen die vom Deutschen Wetterdienst (DWD) herausgegebenen Hochwasserwarnungen (für sich) richtig interpretieren kann, hängt u. a. davon ab, wie gut ausgebildet das zuständige Personal vor Ort ist. Der DWD informiert lediglich über Zahlen, wie z. B. zu erwartende Hochwasserstände, nicht über die daraus potentiell resultierenden Probleme für einzelne Akteur*innen.

Klinger et al. stellten fest, dass es keine einheitlichen Regelungen bezüglich der **Initiierung** von Krisenstäben während der COVID-19-Pandemie gab [16]. Es wurden 43 Krisenstäbe in 14 Bundesländern untersucht, auf Landes-, Bezirksregierungs- und Landkreis- bzw. Kommunalebene, sowie auf Ebene der Einrichtungen der Gesundheitsversorgung (z. B. Krankenhäuser, Hospize oder Alten- und Pflegeheime).

Die Festlegung von Schwellenwerten zur Initiierung des Krisenmodus könnte grundsätzlich natürlich hilfreich sein, einerseits, um die ggfs. unterschiedlichen Ausbildungsstände der zuständigen Krisenmanager*innen auszugleichen und andererseits, um bei flächendeckenden Krisen eine einheitliche Vorgehensweise zu erleichtern (z. B. könnten Abstimmungen zwischen regionalen Krisenstäben von Beginn an erfolgen).

Praktisch scheitert dies jedoch in vielen Fällen an zwei Hürden: (1) der Vielzahl der Faktoren, die dazu führen, dass ein Ereignis als Krise bezeichnet werden kann oder sich zu einer Krise entwickelt, sowie (2) den unterschiedlichen Auswirkungen ebenjenes Ereignisses auf die verschiedenen Behörden bzw. Betreiber kritischer Infrastrukturen. Für ein Hochwasserereignis kann also zum Beispiel gesagt werden:

ob ein prognostizierter Pegelstand eintritt und für wen dieser Pegelstand dann als „kritisch“ einzustufen ist, ist durch einen einfachen Schwellenwert oft nicht festzulegen.

Auf lokaler, also kommunaler Ebene könnten Schwellenwerte in einigen Fällen festgelegt werden, z.B. im Rahmen der Erstellung eines KRITS-Katasters, eines Katastrophenschutz(bedarfs)planes, Hitzeschutzplanes ö. ä., wenn viele beteiligte Akteur*innen in Workshops oder „runden Tischen“ zusammenkommen, Szenarien durchsprechen und über Abhängigkeiten und benötigte Informationen, Ressourcen etc. sprechen. Dies ist nach Einschätzung der Autorin jedoch nicht oder nur schwer und mit großen Unsicherheiten auf die Landesebene übertragbar und gilt zudem eher für Extremwetter- (z.B. durch sehr detaillierte Starkregenkarten) als für pandemische Ereignisse. Trotz der spätestens seit der COVID-19-Pandemie bekannten Indikatoren wie Inzidenz, Intensivbettenbelegung/Hospitalisierungsrate, Impfquote, Todesfälle etc., wird ein potentielles „neues“ Virus zumindest zu Beginn aller Wahrscheinlichkeit nach zu viele unbekannte Parameter aufweisen, als dass diese Indikatoren vorab in sinnvolle Schwellenwerte gemünzt werden können.

2.3 Wie wappnen sich die kritischen Infrastrukturen auf zukünftige Krisenereignisse? Welche Rolle wird in diesem Rahmen dem Bund, dem Land NRW und den Kommunen zuteil? Sind die derzeitigen regulatorischen Vorgaben ausreichend oder müssten diese implementiert/geändert/angepasst werden?

Die konkrete **Vorbereitung** auf künftige Krisenereignisse obliegt den einzelnen Betreiber kritischer Infrastrukturen im Zuge ihres Risiko- und Krisenmanagements und entzieht sich im Einzelnen der Kenntnis der Autorin. Auf kommunaler Ebene sind der Autorin einige Beispiele bekannt, bei denen Betreiber kritischer Infrastrukturen (konkret die Feuerwehr und ein Verteilnetzbetreiber) eigene Maßnahmen ergreifen, um die Sicherheit und Verfügbarkeit ihres Personals zu erhöhen. Dies beinhaltet z. B. das Bevorraten von ausreichenden Lebensmitteln und Wasser auch für Familienangehörige oder die Kooperation mit städtischen Kinderbetreuungseinrichtungen.

Dem **Bund** kommt über das BBK und seine unterstützende Funktion im Bevölkerungs- und Katastrophenschutz z.B. in Teilen die Ausbildung zu. Die in 2.1 genannte Ausweitung der Kapazitäten für Schulungen unternehmerischer Krisenstäbe, konkret das Modul „Risiko- und Krisenmanagement für KRITIS-Betreiber“ der BABZ ist ein Indiz dafür, dass hier ein Mangel erkannt wurde. Ob dieses Modul jedoch in der Folge auch stärker angefragt und absolviert wird, ist der Autorin nicht bekannt.

Der Bund hat des Weiteren beschlossen, ein „Gemeinsames Kompetenzzentrum Bevölkerungsschutz“ (GeKoB) aufzubauen, um die Zusammenarbeit von Bund und Ländern zu vereinfachen und zu stärken [15]. Hier werden dauerhaft Bund, Länder und weitere Akteur*innen (z.B. Hilfsorganisationen) an der Erarbeitung eines „Lagebildes Bevölkerungsschutz“ arbeiten und mit diesem auch während krisenhafter Ereignisse die Krisenstäbe auf Bundes- und Länderebene unterstützen. Die Einbindung von Betreibern kritischer Infrastrukturen ist nach Kenntnis der Autorin nicht geplant. Das GeKoB hat seine Arbeit aufgenommen.

Im Zuge eines geplanten Ausbaus von strategischen Reserven wie Öl, Gas und Nahrungsmittel soll geprüft werden, ob der Bund die Betreiber kritischer Infrastrukturen unterstützen kann, indem auf nationaler Ebene Notstromaggregate bevorratet werden, die im Krisenfall bei der Aufrechterhaltung kritischer Dienstleistungen unterstützen können [15].

Bereits während des katastrophalen Hochwassers im Juli 2021 konnten bundeseigene mobile Trinkwassertransportsysteme genutzt werden. Die positive Evaluation dieses Einsatzes hat dazu geführt, dass „künftig“ [15] weitere solcher modularen Systeme zur Verfügung stehen sollen. Geplant

ist außerdem ein Expert*innennetzwerk für den Sektor Wasser, welches die Einsatzleitungen in Krisengebieten in Zukunft unterstützen soll [15].

In **NRW** gibt es des Weiteren den „Runden Tisch zur Verwundbarkeit durch langanhaltenden und großflächigen Stromausfalls“ [18]. Empfehlungen aus diesem Gremium waren u. a. die Identifizierung und Priorisierung aller als kritischer Infrastruktur anzusehenden Sektoren und Branchen sowie die Erarbeitung von Möglichkeiten und Maßnahmen zur Erhöhung der Resilienz in Zusammenarbeit der verantwortlichen Ressorts, kommunale Verbände und weiterer Beteiligter.

Im Abschlussbericht zur Hochwasserkatastrophe finden sich im Kapitel „Ausblick“ auch Maßnahmen, die NRW im Anschluss im Zuge von „lessons to learn“ umgesetzt hat und die in Teilen kritische Infrastrukturen betreffen.

Es wurde u. a. ein „Kompetenzteams Katastrophenschutz“ berufen, dessen Aufgabe es u. a. war, sich mit Szenarien zu befassen, die den Ausfall kritischer Infrastrukturen beinhalten. Der Abschlussbericht dieses Kompetenzteams liegt vor [17] und enthält für KRITIS folgende Empfehlung: „Das bedeutet konkret, dass für sämtliche KRITIS-Einrichtungen Notfallpläne für denkbare Katastrophenszenarien zu erstellen, mit den örtlichen Katastrophenschutzbehörden abzustimmen und in regelmäßigen Abständen zu überarbeiten und zu üben sind.“

Die Empfehlungen des „Runden Tisches“ (s. o.) haben auch direkten Bezug zur Rolle der **Kommunen**. Diese hätten durch die notwendige Abstimmung einen Überblick über die kritischen Infrastrukturen in ihrer Zuständigkeit. So ein - auch KRITIS-Kataster genannter - Überblick existiert bereits in einigen Kommunen, der Anteil an NRW-Kommunen mit einem solchen sowie die Qualität dieser Kataster im Einzelnen sind der Autorin jedoch nicht bekannt.

Inwieweit diese Empfehlung und auch die weiteren oben genannten Maßnahmen und Empfehlungen des Bundes und Landes bereits umgesetzt wurden, ist der Autorin ebenfalls nicht bekannt.

Entsprechend der hier aufgezählten Maßnahmen und Empfehlungen des Bundes und NRWs scheint deutlich zu werden, dass die Risiken, die viele Krisenszenarien für kritische Infrastrukturen beinhalten, in weiten Teilen bekannt sind und auch, dass entsprechende Maßnahmen zur Vorbereitung essentiell sein können (z. B. die Vorhaltung von Notstromaggregaten bzw. einer Priorisierung der Verteilung dieser, das Beüben von Szenarien und Meldewegen, institutionalisierte Kooperationen zwischen Bund, Ländern und KRITIS-Betreibern etc.). Sowohl aus der Gesetzgebung heraus als auch aus Empfehlungen und länderspezifischen Maßnahmen ergeben sich dementsprechend ausreichend Möglichkeiten der Resilienzstärkung von KRITIS-Unternehmen.

Die Umsetzung der Erkenntnisse in konkrete Maßnahmen (wie z.B. die erfolgreiche Einrichtung des GeKoB) ist allerdings noch nicht flächendeckend erfolgt und sollte daher künftig an erster Stelle stehen.

2.4 Wie ist im Bereich KRITIS die Kommunikationsstruktur auf EU-, Bundes-, Länder und kommunaler Ebene organisiert?

Unter 1.3 a) wurden das Benennen einer Kontaktstelle (zum BSI) sowie die Melde- und Nachweispflicht als einige der Pflichten von KRITIS-Betreibern, die sich aus dem BSIG ergeben, genannt. Wie genau die Kommunikation zwischen dem BSI und diesen Kontaktstellen aussieht, entzieht sich der Kenntnis der Autorin, ebenso die konkrete Ausgestaltung der weiteren in der Frage genannten Kommunikationsstrukturen.

2.5 Gibt es dort aus Ihrer Sicht Verbesserungsbedarf und wenn ja, was empfehlen Sie?

Der Entwurf des KRITIS-Dachgesetzes als nationale Umsetzung der europäischen CER-Richtlinie beinhaltet sowohl nationale Melde- und Kommunikationswege, als auch solche in Richtung der EU. Wie diese konkret aussehen, wird jedoch erst mit Verabschiedung dieses Gesetzes feststehen. Es besteht also die Chance, die Kommunikationswege an dieser **Stelle transparent, einheitlich** und für die Betreiber möglichst **einfach** zu gestalten.

Hinzu kommen hier auch noch ggfs. sich ändernde Meldepflichten und Kommunikationswege durch das NIS2-Umsetzungsgesetz, welches analog zum KRITIS-DachG ebenfalls in diesem Jahr in Kraft treten soll. Die (gemeinsame) Registrierung bei entsprechenden Behörden mit dem KRITIS-Dachgesetz ist noch nicht geklärt.

Die Chance zur Vereinheitlichung sollte an dieser Stelle dringend genutzt werden.

2.6 Wie ist die Vulnerabilität kritischer Infrastrukturen einzuschätzen?

Nach Einschätzung der Autorin sind sich zumindest die Betreiber der nach BSI-KritisV definierten kritischen Infrastrukturen ihrer Rolle und Kritikalität bewusst. Die Pflichten nach BSIG tragen dazu bei, dass dieses Bewusstsein geschärft wird und das Risiko- und Krisenmanagement kontinuierlich weiterentwickelt wird.

Eine unterschätzte – oder besser gesagt von den Betreibern oft nur schwer zu adressierende – Problematik sind nach Einschätzung der Autorin die wechselseitigen **Abhängigkeiten** kritischer Infrastrukturen untereinander. Die europäische CER-Richtlinie trägt der Notwendigkeit Rechnung, *europaweite* Abhängigkeiten kritischer Infrastrukturen stärker in den Fokus zu rücken. Durch die in der Richtlinie angestrebte Harmonisierung von Maßnahmen und Vorgaben zum Schutz kritischer Infrastrukturen in Europa können sich jedoch auch jetzige nationale Gegebenheiten ändern, weitere Einrichtungen zur kritischen Infrastruktur gezählt werden und neue Meldewege und Pflichten hinzukommen. Die Inkludierung nationaler Abhängigkeiten in individuellen Risikoanalysen ist nach Einschätzung der Autorin notwendig – wenn nicht bereits geschehen –, um die Voraussetzung für die Analyse internationaler Abhängigkeiten zu schaffen.

In diesem ersten Punkt klang bereits eine weitere Problematik an: nicht alle für das Wohlergehen der Bevölkerung kritischen Einrichtungen sind auch KRITIS nach BSI-KritisV. Ob und inwieweit sich der Kreis durch das KRITIS-DachG erweitern wird, lässt sich noch nicht abschließend beurteilen. Die Notwendigkeit und bereits jetzt gegebene Möglichkeit, angepasste Schwellenwerte zu nutzen um regional sinnvolle KRITIS-Kataster zu erstellen, wurde in 1.1, 1.3 und 1.4 bereits genannt und beschrieben. Da dies aber weder flächendeckend geschieht, noch die entsprechenden Pflichten nach BSIG nach sich zieht, ist davon auszugehen, dass es deutschlandweit viele Einrichtungen und Organisationen gibt, **die sich ihrer Kritikalität nicht oder nicht in vollem Umfang bewusst sind**. Diese Einrichtungen werden in der Folge unter Umständen auch kein ihrer Kritikalität angemessenes Risiko- und Krisenmanagement haben und sind dadurch ggfs. vulnerabler und weniger widerstandsfähig.

2.7 Inwieweit stehen die Mitarbeitenden kritischer Infrastrukturen unter besonderem Schutz? Gibt es in diesem Bereich Handlungsbedarf?

Allgemeine Vorgaben zum Schutz des Personals in kritischen Infrastrukturen sind der Autorin nicht bekannt. Das Beispiel des NRW-Leitfadens zur Bestimmung des Personals kritischer Infrastrukturen [9] macht deutlich, dass krisenspezifische Lösungen möglich sind.

Unter Punkt 2.3 (1. Absatz) sind Beispiele für betreibereigene Maßnahmen zum Schutz bzw. der verbesserten Verfügbarkeit ihres Personals genannt. Es ist davon auszugehen, dass es neben diesen noch weitere Beispiele gibt, die sich jedoch der Kenntnis der Autorin entziehen.

2.8 Welche Erkenntnisse bzgl. der Mitarbeitenden konnten aus der pandemischen Lage gewonnen werden und im wieweit werden diese bereits umgesetzt bzw. sollten umgesetzt werden?

Der Autorin ist keine Evaluation der Umsetzung bzw. Wirksamkeit und Effizienz des NRW-Leitfadens zur Bestimmung des Personals kritischer Infrastrukturen bekannt. Falls es eine solche Evaluierung noch nicht gibt, wäre sie sinnvollerweise zu erstellen, um daraus Schlüsse für künftige Lagen ziehen zu können.

Im Zuge der Verbreitung der hochansteckenden Omikronvariante des COVID-19 Virus kamen an vielen Stellen, vor allem auch in den Medien, Befürchtungen auf, dass kritische Infrastrukturen aufgrund eines akuten Personalmangels ausfallen könnten. Ein Beispiel für ein konkret eingetretenes Problem ist die Deutsche Bahn, die zeitweise kürzere Züge fahren lassen musste, um die Instandhaltungswerke zu entlasten. Beispiele für Medienbeiträge zu dem Thema sind [19, 20, 21].

Viele Betreiber haben sich im Rahmen ihrer Möglichkeiten auf ein solches Szenario vorbereitet, z. B. durch die Trennung von Personal unterschiedlicher Schichten um die Ansteckungsgefahr zu reduzieren oder der Planung von im Notfall einsetzbaren „Infizierten-Schichten“ [22].

Eine Aufweichung der zu der Zeit gültigen Quarantänevorschriften wurde ebenfalls diskutiert, z. B. die Verkürzung der Quarantänezeit oder die Arbeitserlaubnis für symptomlos infizierte Mitarbeiter*innen kritischer Infrastrukturen.

Die Beispiele zeigen, dass es ein hohes Bewusstsein der Problematik bei den Beteiligten gab und dementsprechend unterschiedliche – auch ungewöhnliche und ggfs. drastische – Maßnahmen angedacht wurden. Zum Glück ist der befürchtete KRITIS-Personalmangel nur sehr vereinzelt eingetreten (von dem chronischen Personalproblem in Krankenhäusern und dessen Verstärkung während der Coronawellen mal abgesehen). Daher konnte nach Einschätzung der Autorin keine Evaluierung der angedachten Maßnahmen stattfinden, anhand der nun entsprechende Erkenntnisse für zukünftige pandemische Lagen abgeleitet werden könnten.

2.9 Welche Auswirkungen wird das neue KRITIS-Dachgesetz auf den Bevölkerungs- und Katastrophenschutz in NRW voraussichtlich haben?

Einleitend ist zu sagen, dass der Entwurf des KRITIS-Dachgesetzes (Stand vom 21.12.2023) vorsieht, die Synergien zum BSIG wo immer sie möglich und sinnvoll sind zu nutzen. Dies bedeutet z. B., dass Betreiber kritischer Infrastrukturen Störungsmeldungen im Sinne des BSIG oder des KRITIS-DachG in Zukunft wohl auf einer gemeinsamen digitalen Plattform des BSI und des BBK melden können. Es sollen des Weiteren Schnittstellen zwischen IT-Sicherheit (geregelt im BSIG) und „physischer Sicherheit“ (in Zukunft geregelt durch das KRITIS-DachG, hier als vereinfachter Ausdruck des „All-Gefahren-Ansatzes“) berücksichtigt und Regelungen wenn möglich angeglichen werden.

Das führt im besten Falle dazu, dass Betreiber kritischer Infrastrukturen zwar einen erweiterten Ansatz bei ihren Risikoanalysen und -bewertungen berücksichtigen müssen, sie jedoch wo immer möglich gleiche oder ähnliche Methoden anwenden sowie Resilienzmaßnahmen „übereinstimmend ausgestalten“ können [7].

§3, Absatz 4 des Entwurfs des KRITIS-DachG vom 21.12.2023 beinhaltet die Vorgabe für die Bundesländer, „eine Landesbehörde als zentralen Ansprechpartner für sektorenübergreifende Angelegenheiten im Zusammenhang mit der Durchführung dieses Gesetzes“ zu benennen [7].

Weiter soll es auf Bundesebene das BSI für den Sektor Informationstechnik und Telekommunikation, die Bundesnetzagentur für den Sektor öffentliche Telekommunikationsnetze, die Bundesanstalt für Finanzdienstleistungsaufsicht für den Sektor Finanz- und Versicherungswesen sowie ggf. weitere Aufsichtsbehörden geben. Für alle nicht unter bereits bestehende Aufsichtsbehörden fallenden Sektoren sowie für die übergeordneten, branchen- und sektorübergreifenden Aufgaben soll das BBK zuständig sein. Das Gesetz soll den Informationsaustausch zwischen den aufsichtführenden Behörden auf Länder- und Bundesebene regeln und damit u. a. eine frühzeitige Alarmierung potentiell durch eine Störungsmeldung betroffener weiterer Betreiber ermöglichen.

Diese so gegebenenfalls verbesserte behördliche Zusammenarbeit könnte zu einer **effektiveren Koordination von Ressourcen und Maßnahmen im Katastrophenfall** führen. Ein weiterer Aspekt sind sektorspezifische Mindestanforderungen, die von den aufsichtführenden Behörden und/oder Branchenverbänden festgelegt werden sollen und die dementsprechend eine **einheitliche Herangehensweise an den Schutz kritischer Infrastrukturen** anstreben. Es ist eher unwahrscheinlich, dass alle Betreiber kritischer Infrastrukturen in NRW diesen Mindeststandards bereits genügen werden, was in der Folge zu einer Erhöhung der Resilienz führen sollte. Die Durchführung staatlicher Risikoanalysen und -bewertungen für kritische Dienstleistungen soll einen **Gesamtüberblick über die Risiken bieten und Betreiber bei ihren Maßnahmen unterstützen**. Dies könnte zu einer besseren Vorhersage und Bewältigung potenzieller Krisen führen.

Diese potentiell positiven Auswirkungen des KRITIS-Dachgesetzes setzen voraus, dass die Umsetzung der Vorgaben des Gesetzes und seiner aller Voraussicht nach folgenden konkretisierenden Rechtsverordnungen effektiv überwacht und durchgesetzt werden. Hier werden entsprechende Stellen des Landes ebenso gefragt sein, wie Bundesbehörden. Vorgesehener Stichtag für die Benennung eines zentralen Ansprechpartners für sektorübergreifende Angelegenheiten ist zur Zeit der 02.01.2025.

Zwei weitere Aspekte des KRITIS-Dachgesetzes werden **voraussichtlich Auswirkungen auf NRW** haben. Zum einen kann das BMI auf Betreiben der zuständigen Aufsichtsbehörden des Bundes und der Länder unter Berücksichtigung der nationalen Risikoanalysen und Risikobewertungen Betreiber kritischer Anlagen identifizieren, die bisher, nach Definition des BSIG, nicht als kritische Infrastruktur gelten (§4 (2)). Und zum anderen gibt die CER-Richtlinie vor, das besondere Maßnahmen von Betreibern getroffen werden müssen, deren kritische Dienstleistungen in mindestens sechs weiteren EU-Staaten so oder ähnlich erbracht werden (§7 (1)) oder die anderweitig „von besonderer Bedeutung für Europa“ sind (§7 (2)).

Die angestrebte Verbesserung der Resilienz kritischer Infrastrukturen und die damit einhergehende Verbesserung des Bevölkerungs- und Katastrophenschutzes wird also sowohl auf Betreiberseite, als auch auf Seiten der zuständigen Landesbehörden aller Wahrscheinlichkeit nach zu einem **erhöhtem administrativen und operativen Aufwand** führen:

- Ggfs. mehr Betreiber als bisher erfüllen die Kriterien, die sie als kritische Infrastruktur ausweisen

- Diese und einige der bereits als KRITIS definierten Betreiber werden Risikoanalysen, Risikobewertungen und - nach Kenntnis der Autorin neu, im Sinne von nicht verpflichtend nach BSIG - Resilienzpläne erstellen bzw. ihre vorhandenen anpassen müssen
- Die daraus abzuleitenden zusätzlichen Maßnahmen zur Erhöhung der physischen Sicherheit werden aller Voraussicht nach Kosten nach sich ziehen
- Betreiber und Behörden werden einen erhöhten Kommunikationsaufwand haben und ggfs. Personal zur Verfügung stellen müssen
- Schulungs- und Berichtspflichten stellen ebenfalls einen erhöhten Aufwand dar

Die **Zeitspannen**, die KRITIS-Betreiber dabei zur Verfügung stehen, sind verhältnismäßig kurz: für die Registrierung einer Anlage beim BBK sind bisher drei Monate vorgesehen, ab dem Zeitpunkt zu dem festgestellt wird, dass eine Anlage unter das Gesetz fällt (§6 (1)). Nach der Registrierung stehen dann neun Monate für die Erstellung von Risikoanalysen und -bewertungen im Sinne des Gesetzes zur Verfügung und 10 Monate für die Erstellung von Resilienzplänen sowie der Beteiligung am Störungsmeldewesen (§7 (6)).

In Abschnitt VI „Gesetzesfolgen“, Unterabschnitt 4, „Erfüllungsaufwand“, Absatz c „**Erfüllungsaufwand für die Verwaltung**“ sind folgende die verantwortlichen Landesbehörden betreffende Aspekte genannt, die Personal- und Sachkosten beinhalten (die angegebenen Paragraphen sind jeweils aus dem Referentenentwurf des KRITIS-DachG vom 21.12.2023):

- Erarbeitung einer nationalen KRITIS-Resilienzstrategie nach §1
- Durchführung von nationalen Risikoanalysen und -bewertungen nach §8
- Erarbeitung von sektorübergreifenden Mindestanforderungen und branchenspezifischen Resilienzstandards nach §10
- Nachweisverfahren zu Maßnahmen zur Sicherung der physischen Resilienz nach §11
- Bearbeitung von Anträgen auf Äquivalenzprüfung nach §§9 bis 11 in Verbindung mit §4
- Mitteilungs-, Veröffentlichungs- und Berichtspflichten nach §§3, 7 und 15
- Durchführung von Ordnungswidrigkeitsverfahren nach §19

In der **„Länderabgestimmten Stellungnahme“** des AK V „Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung“ der Ständigen Konferenz der Innenminister und -senatoren der Länder [23] wird bemängelt, dass bisher weder der Sektor „Staat und Verwaltung“, noch die Sektoren „Medien und Kultur“ sowie „Sozialwesen“ als potentielle KRITIS-Sektoren nach KRITIS-DachG gelten. Die ersten beiden sind schon einmal – abweichend von der BSI-Definition – durch die Bundesländer in Form der Bund-Länder AG in die nationalen KRITIS-Sektoren aufgenommen worden, der kritische Hinweis auf ihr Fehlen im KRITIS-DachG ist also aus ihrer Sicht und der der Autorin nur folgerichtig.

Ein weiterer Punkt in dieser Stellungnahme bezieht sich auf die im Referentenentwurf des KRITIS-Dachgesetzes unter §10 genannten Resilienzmaßnahmen. Hier wird bemängelt, dass diese sich nicht konkret auf die Phasen des Risiko- bzw. Krisenmanagementzyklus beziehen (Prävention – Vorbereitung – Bewältigung – Nachsorge), sondern eher vage bleiben. Der konkrete Bezug zu den Phasen böte für die Akteur*innen im Bevölkerungsschutz (auch des Landes) den Vorteil der direkten Übertragbarkeit und Anwendbarkeit auf ihre Maßnahmen.

3. Bevölkerung

3.1 und 3.2 Welche Rolle spielt die Bevölkerung für die Resilienz kritischer Infrastrukturen? Welche Rolle spielt die Resilienz der Bevölkerung für die Sicherheit von kritischen Infrastrukturen?

Da die Unterscheidung der Fragen 3.1 und 3.2 nach Einschätzung der Autorin schwierig ist, werden im Folgenden beide Fragen gemeinsam beantwortet.

Die Handlungen und Verhaltensweisen der Bevölkerung können einen erheblichen Einfluss darauf haben, wie schnell und effektiv auf eine Krise reagiert werden kann. Ein verantwortungsbewusstes Verhalten, das die Ressourcen schont und die Sicherheit aller gewährleistet, kann dazu beitragen, die **Auswirkungen von Störungen auch in kritischen Infrastrukturen zu minimieren**. Dies kann z. B. den sparsamen Umgang mit Wasser bedeuten, wenn dieses nicht mehr durch vorhandene Netze, sondern mittels mobiler Lösungen bereitgestellt wird, da so eine bessere Planbarkeit und längere Versorgungsmöglichkeit gegeben sind. Ein weiteres Beispiel stellt der **verantwortungsvolle Umgang** mit Informationen dar, welcher die polizeiliche Gefahrenabwehr nicht durch Desinformationen und sich daraus ggfs. ergebendem Fehlverhalten zusätzlich beansprucht. Dies beinhaltet aber auch die verantwortungsvolle Verwendung des Notrufs (nur in echten Gefahrensituationen) und des Handynetzes, welches potentiell durch ausgefallene Masten nur eingeschränkte Kapazitäten hat. Weitergehend stellt auch die Reduzierung der Nutzung von PKWs auf nur zwingend erforderliche/notwendige Fahrten ein verantwortungsbewusstes Verhalten dar, welches Verkehrswege für Einsatzkräfte potenziell freihält. Die Einhaltung von Evakuierungsanweisungen, die Sicherung von Gegenständen im Freien, das Abschalten von Gasleitungen oder die Bereitstellung von Erste-Hilfe-Maßnahmen können ebenfalls Leben retten und die Auswirkungen der Krise minimieren.

Die zielgruppengerechte Aufklärung der Bevölkerung muss sowohl auf Bundes- als auch auf Landes- und Kommunalebene erfolgen. Hier sind Konzepte und Formate wichtig, die über Broschüren hinausgehen, z. B. städtische Katastrophenschutztage, der nationale „Tag des Bevölkerungsschutzes“, oder gezielte Aufklärungskampagnen.

3.3 Welche Erkenntnisse liegen im Rahmen der Risiko- und Krisenkommunikation in Richtung der Bevölkerung vor? Hat die Pandemie diese Erkenntnisse beeinflusst und wenn ja, inwiefern?

Für die unter 3.1 und 3.2 genannten Aspekte ist ein grundlegendes **Verständnis der Bevölkerung für das Verhalten in Krisensituationen** wichtig. Dieses Verständnis hat eine nicht zu unterschätzende Auswirkung auf die Resilienz der Bevölkerung, denn nur informierte Bürger*innen können sich angemessen vorbereiten. Von besonderer Relevanz ist hierfür eine gute und angepasste Risiko- und Krisenkommunikation, welche allerdings vor allem durch die Heterogenität unserer Gesellschaft eine Herausforderung darstellt [24].

Retrospektiv erscheint der Ansatz von Sandman [25] im Zusammenhang mit Epidemien und/oder Pandemien passend und anwendbar: der Autor postuliert, dass die **Akzeptanz von Risiken** von zwei Schlüsselkomponenten geprägt ist: Gefahr (hazard) und Empörung oder Entsetzen (outrage). Die Anzahl der Menschen, die exponiert, infiziert und erkrankt sind, kann dabei als die „Gefahr“ betrachtet werden. Wie die Öffentlichkeit auf Botschaften zur Risikominderung reagiert, hängt mit der „Empörung“ oder dem „Entsetzten“ zusammen. Soziale und kulturelle Faktoren, Dringlichkeit, Unsicherheit, Vertrautheit, persönliche Kontrolle, wissenschaftliche Unsicherheit und das Vertrauen in Institutionen und Medien prägen dementsprechend alle die Wahrnehmung und Reaktion der Bevölkerung auf Risikobotschaften [26].

Die zentrale Rolle, die die wissenschaftliche Unsicherheit und das Vertrauens in Institutionen und Medien (beides Aspekte, die direkt und indirekt Personen sowie Institutionen des Bundes und Landes betreffen) in Deutschland und natürlich auch NRW während der COVID-19-Pandemie gespielt haben, ist offensichtlich. Insbesondere die Kommunikation neuer und ggfs. vorherigen Anweisungen und

Sprechweisen widersprechenden (hier z. B. medizinischer/epidemologischer) Erkenntnisse stellt hierbei eine Schwierigkeit dar.

3.4 Welche Erkenntnisse gab es nach der Coronapandemie und den nationalen Warntagen in Bezug auf die Risikokommunikation und -wahrnehmung?

2022 ist beim **nationalen Warntag** erstmals Cell Broadcast genutzt worden, bei dem Warnnachrichten direkt auf das Handy oder Smartphone geschickt werden. Über weitere sogenannte Warnmultiplikatoren des MoWaS (Modulares Warnsystem des Bundes) wurden ebenfalls Warnungen ausgegeben, z. B. die Warn-Apps NINA, KATWARN und BIWAPP, zahlreiche Medienanstalten, Fahrgastinformationssysteme an Bahnhöfen und Haltestellen sowie das zentrale Warnportal *www.warnung.bund.de*. Darüber hinaus wurden kommunale Warnmöglichkeiten wie Sirenen eingebunden. In der anschließend vom BBK durchgeführten deutschlandweiten Umfrage gaben über 90 Prozent der Befragten an, über mindestens einen Kanal gewarnt worden zu sein [27]. Die entsprechenden Erkenntnisse über den Warntag 2023 stehen noch aus.

Eine weitere Erkenntnis des Warntages ist, dass knapp 10 Prozent der Befragten ausschließlich über Cell Broadcast gewarnt wurden. Die Einkommens- und Verbrauchsstichprobe (EVS) des Statistischen Bundesamtes von 2018 besagt, dass 96,7 Prozent der Haushalte im Besitz mindestens eines Mobiltelefons ist, darunter 77,9 Prozent Smartphones [27b]. Laut statista.de nutzten im Jahr 2022 schon 81,1 Prozent der Bevölkerung Smartphones. Die Tatsache, dass also fast jede*r ein Handy oder sogar Smartphone besitzt, kann sich dementsprechend in einer Krise als überaus nützlich für die Kommunikation erster Informationen erweisen. Für pandemische Ereignisse eignet sich diese Form der Krisenkommunikation (zumindest dauerhaft, z. B. für die Information über Maßnahmenupdates etc.) jedoch eher nicht.

Zwei Drittel der Befragten empfinden einen nationalen Warntag als sinnvoll. Dies ist bei über 800.000 verwertbaren ausgefüllten Fragebögen ein deutlicher Hinweis darauf, dass die Bevölkerung die Sinnhaftigkeit von Warnungen im Grundsatz nicht infrage stellt. Problematisch hingegen ist der Umstand, dass die Freiwilligkeit der Befragung aller Wahrscheinlichkeit nach eine eingeschränkte Repräsentativität der Ergebnisse zur Folge hat: von den Befragungsteilnehmer*innen könnten sich überdurchschnittlich viele Personen durch ein grundsätzliches Interesse am Thema Warnung/Krisenkommunikation auszeichnen, da sie auf den Fragebogen aufmerksam wurden und sich die bewusst Zeit genommen haben, diesen zu beantworten.

Bezogen auf den abschließenden Absatz zu Fragen 3.1 und 3.2 ist des Weiteren zu sagen, dass der nationale Warntag mit seinen begleitenden Informationen ein wichtiger Baustein in Bezug auf die Aufklärung der Bevölkerung sein kann und dafür genutzt werden sollte.

3.5 Wo lagen aus Ihrer Sicht Probleme in der Krisenkommunikation?

Wie bereits in 3.3 dargestellt wurde, haben die wissenschaftliche Unsicherheit und die damit einhergehenden, häufig zu kommunizierenden neuen Erkenntnisse sowie abzuleitenden Maßnahmen eine zentrale Problematik der Krisenkommunikation dargestellt. Dies führte in der Bevölkerung teilweise zu Verunsicherung und Überforderung, welche wiederum die Neigung erhöhen, vermeintlichen einfachen „Lösungen“ glauben zu schenken. Diese Lösungen sahen z. B. die unkontrollierte Ausbreitung des Virus vor, da es Quellen gab, die keine schlimmeren Auswirkungen als eine Grippe bei einer COVID-19-Infektion prognostizierten, obwohl die Zahlen der Intensivbettenbelegung und die zeitweise langen Anfahrtswege zu entsprechend ausgestatteten Intensivbetten anderes belegten. Angekündigte und in Kraft getretene Maßnahmen wurden diffamiert

und als unnötig dargestellt. Der Wikipedia-Artikel „Falschinformationen zur COVID-19-Pandemie“ listet für Deutschland nachprüfbare „Fake News“ auf, z. B. den Grippevergleich, die Eingrenzung der Gefahr auf bestimmte Bevölkerungsgruppen oder die Meldung, dass das Virus gar nicht existiert [28].

Unterschiedliche Maßnahmenpakete in den Bundesländern trugen ebenso dazu bei, der Bevölkerung ein uneinheitliches Bild zu vermitteln wie die mediale Berichterstattung an einigen Stellen. Politische Maßnahmen können nicht alleine auf wissenschaftlichen Erkenntnissen beruhen, da hier viele Faktoren berücksichtigt werden müssen, die in der Wissenschaft oft nur eine untergeordnete Rolle spielen (z. B. gesellschaftliche Auswirkungen, Machbarkeit, Konsensfähigkeit etc.). Wenn jedoch ein sehr breiter wissenschaftlicher Konsens vorhanden ist, tragen Medien, die um der Diskussion willen unterschiedliche, möglichst konträre „Seiten“ hören und zu Wort kommen lassen wollen, zu einer sogenannten „false balance“ bei [29]. Wenn z. B. 90 % der wissenschaftlichen Artikel und Forschung zu einem Thema ungefähr einer Meinung ist und 10 % sind anderer, wird dieses Verhältnis bei einer Diskussion zwischen einer Wissenschaftlerin der „einen Seite“ und einer Wissenschaftlerin der „anderen Seite“ nicht wiedergegeben. Den Zuschauer*innen, Hörer*innen und Leser*innen, also der Bevölkerung, wird eine in der Form nicht existierende Uneinigkeit der Wissenschaft präsentiert.

3.6 und 3.7 Inwieweit beeinträchtigen „Fake News“ die Arbeit der kritischen Infrastrukturen? Inwieweit beeinträchtigen Desinformationskampagnen die Arbeit der kritischen Infrastrukturen?

Laut Bundeszentrale für politische Aufklärung ist Desinformation „absichtlich irreführend, verfolgt also eine Agenda“ und der Begriff wird im weitesten Sinne synonym zu „Fake News“ genutzt [30]. Ausgehend von dieser bedeutungsgleichen Definition werden die Fragen zur Beeinträchtigung kritischer Infrastruktur durch „Fake News“ sowie Desinformationskampagnen folgend zusammen beantwortet.

Unter 3.5 wurden bereits Problematiken, die durch die Verbreitung von „Fake News“ entstehen können, genannt. Konkret auf die Arbeit kritischer Infrastrukturen bezogen, kann sich Desinformation unterschiedlich auswirken. Im Folgenden einige Beispiele, wie "Fake News" zu Fehlalarmen, Ressourcenverschwendung und Beeinträchtigungen der ordnungsgemäßen Funktion kritischer Infrastrukturen führen könnten, was letztendlich die Fähigkeit der Gesellschaft beeinträchtigt, auf reale Krisen angemessen zu reagieren und sich davon zu erholen:

Energieversorgung: Falsche Informationen über angebliche Stromausfälle oder Versorgungsengpässe können Angst in der Bevölkerung auslösen, was zu einem übermäßigen Verbrauch führt und die Kapazität der Stromnetze überlastet. Dies kann zu tatsächlichen Ausfällen führen und die Arbeit der Energieversorgungsunternehmen beeinträchtigen.

Ähnliches gilt auch für die **Telekommunikation**: Falsche Berichte über angebliche Störungen oder Schwachstellen in Telekommunikationsnetzen können zu einem übermäßigen Anruf- und Datenverkehr führen, der die Netzwerkinfrastruktur überlastet und die Kommunikation für kritische Dienste wie Notrufe oder Katastrophenmanagement erschwert.

Gesundheitswesen: Falsche Behauptungen über angebliche Heilmittel oder falsche Informationen über die Sicherheit von Impfstoffen können dazu führen, dass Menschen medizinische Ratschläge ignorieren oder sich für unsichere Behandlungen entscheiden. Dies kann zu einem Anstieg der Krankheitsfälle führen und die Kapazität des Gesundheitssystems überfordern.

Wasserversorgung: Falsche Berichte über angebliche Verunreinigungen oder Gefahren für die Wasserversorgung können zu einem übermäßigen Verbrauch von Trinkwasser oder zur Meidung des

Leitungswassers führen, was die Kapazität der Wasserversorgungssysteme belastet und die Lieferung von sauberem Wasser gefährdet.

Transport und Logistik: Falsche Berichte über angebliche Ausfälle oder Engpässe in der Lieferkette können zu einer erhöhten Nachfrage nach bestimmten Gütern führen, was zu Verzögerungen bei der Lieferung wichtiger Güter wie medizinischer Versorgung oder Lebensmitteln führt und die Versorgungskette beeinträchtigt.

3.8 Inwieweit wird das Vertrauen der Bevölkerung in die kritischen Infrastrukturen insgesamt, aber auch bezogen auf die einzelnen Sektoren durch Desinformationskampagnen/“Fake News“ beeinträchtigt? Was können konkret die Auswirkungen davon sein? Welche Maßnahmen empfehlen Sie hier konkret? Welche Akteure sehen Sie hier besonders in der Pflicht?

Die unter 3.7 genannten Beispiele können auch Auswirkungen auf das Vertrauen der Bevölkerung in die entsprechenden kritischen Infrastrukturen haben, vor allem, wenn Vorfälle nicht ausreichend aufgeklärt und entschärft werden (können). Welche Auswirkungen das im Einzelnen oder gesamtgesellschaftlich hat, ist nur schwer abzuschätzen. Auch hier, analog zu den Informationen während der Hochzeiten der COVID-19-Pandemie, spielt die Komplexität der vorliegenden Systeme und ihre wechselseitigen Abhängigkeiten eine große Rolle. Beides führt dazu, dass die Herausforderungen und Risiken der Bevölkerung oft nur schwer zu vermitteln sind. Die Aufgabe von Bundes- und Landesbehörden, aber auch der Betreiber kritischer Infrastrukturen selber muss es sein, dies dennoch, in möglichst verständlicher und zielgruppenangepasster Art und Weise, dauerhaft zu tun.

Im Folgenden sind einige **Maßnahmen** aufgelistet, inkl. der *verantwortlichen Akteur*innen*, die das Vertrauen der Bevölkerung in kritische Infrastrukturen dauerhaft stärken und damit die Resilienz dieser Unternehmen stärken können.

Aufklärung und Bildung: Umfassende Aufklärungskampagnen können helfen, die Öffentlichkeit über die Kritikalität und Relevanz kritischer Infrastrukturen aufzuklären und sie so gegen Desinformation zu immunisieren. Diese Kampagnen können *sowohl von den Betreibern, als auch vom Staat (bzw. dem Land NRW), als auch von beiden gemeinsam* ausgehen.

Transparenz und Kommunikation: *Betreiber kritischer Infrastrukturen* sollten transparent über ihre Arbeitsweise und Sicherheitsmaßnahmen kommunizieren, um das Vertrauen der Öffentlichkeit zu stärken und Desinformationskampagnen entgegenzuwirken.

Förderung kritischer Medienkompetenz: Die Förderung einer kritischen Medienkompetenz in der Bevölkerung kann dazu beitragen, dass Menschen Desinformation erkennen und ihr Vertrauen in verlässliche Informationsquellen stärken. Hier ist der *Staat (bzw. das Land NRW)* in Form von Schulbildung, Fortbildungen der Mitarbeiter*innen im öffentlichen Dienst, gezielten Kampagnen etc. in der Pflicht-

Zusammenarbeit mit Regierungsbehörden: *Regierungsbehörden* sollten mit *Betreibern kritischer Infrastrukturen* im Zuge des Risikomanagements zusammenarbeiten, um Desinformationskampagnen frühzeitig zu erkennen und effektive Gegenmaßnahmen zu ergreifen.

Neben diesen konkreten Maßnahmen können zwei weitere Akteure allgemein dabei unterstützen, dass Desinformation weniger verbreitet und/oder auf eine weniger empfängliche Bevölkerung trifft: Die *Medien* spielen eine wichtige Rolle bei der Verbreitung von Informationen und sollten sich bemühen, zuverlässige und genaue Berichterstattung zu gewährleisten, um Desinformation zu

bekämpfen. Organisationen und Einzelpersonen in der *Zivilgesellschaft*, die in der Bevölkerung Vertrauen genießen, können die Medienkompetenz fördern und die Öffentlichkeit über Desinformationskampagnen aufklären.

3.9 Gibt es weitere Hinweise, die Sie uns für unsere Arbeit geben möchten?

Die Antworten auf die Fragen 1.1 bis 3.8 liefern bereits sehr viele Informationen und Hinweise. Diese Frage soll dazu genutzt werden, einige der wichtigsten Erkenntnisse und Empfehlungen nochmal aufzulisten:

- **KRITIS-Begriff**: Eine Erweiterung des Begriffsverständnisses „kritische Infrastrukturen“ um die Aspekte „Staat und Verwaltung“ sowie „Medien und Kultur“ sowie „Sozialwesen“ auch auf Gesetzesebene, wie es in der Stellungnahme der IMK zum Referentenentwurf zum KRITIS-Dachgesetz gefordert wird, ist empfehlenswert
- **Maßnahmen**: Die Umsetzung von Erkenntnissen aus den unterschiedlichen Gremien (z. B. „Runder Tisch“ in NRW, UP KRITIS, GeKoB, Expert*innengremien zur Aufarbeitung der Flutkatastrophe etc.) in konkrete Maßnahmen sollte vehement verfolgt werden
- **Kommunikation:** Eine Vereinheitlichung und wo nötig Vereinfachung der sich aus den Pflichten der unterschiedlichen Gesetze und Verordnungen ergebenden Kommunikation zwischen KRITIS-Betreibern und Behörden, auf Landes-, Bundes- und europäischer Ebene ist anzustreben
- **Risiko- und Krisenkommunikation:** Die Bereitschaft und die Kapazitäten der Bevölkerung, eigene Krisenvorbereitungen zu treffen und im Krisenfall erwünschte Verhaltensweisen aufzuzeigen, steigt mit dem Wissen um Risiken und die daraus abzuleitenden Konsequenzen und Maßnahmen, sowie mit dem Wissen um die Kapazitäten (und Grenzen) der Akteur*innen im Katastrophenschutz. Hier kann NRW - ggfs. gemeinsam mit den Kommunen – durch gezielte Aufklärung viel erreichen
- **Forschung**: Zu vielen der besprochenen Themen existieren bereits nutzbare Forschungsergebnisse, z. B. in Bezug auf Risiko- oder Krisenkommunikation, Desinformation etc. Weitere Themen und die Vertiefung oder Spezifizierung der zwei genannten Beispiele können durch gezielte Forschung mit wichtigen Erkenntnissen unterfüttert werden
- **Transfer**: es müssen geeignete Strukturen vorhanden sein, damit Forschungsergebnisse (v. a. aus vom Bund oder Land NRW geförderten Projekten) bei den entsprechenden Anwender*innen ankommen

Quellen

[1] BMI, ohne Datum, https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html, zuletzt abgerufen am 09.02.2024

[2] BBK, 2019, Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten, Arbeitshilfe für die Anwendung im Bevölkerungsschutz, Praxis im Bevölkerungsschutz, Band 20

[3] BBK, 2021, Klärung und Erweiterung des KRITIS-Vokabulars; https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/baukasten-kritis-vokabular-1.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 09.02.2024

[4] Vogel, V., Ziegler, N., 2023, Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie, International Cybersecurity Law Review 4:1–19, https://doi.org/10.1365/s43439-022-00077-4

[5] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf, zuletzt abgerufen am 09.02.2024

[6] EU-Parlament, 2022, Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555, zuletzt abgerufen am 20.02.2024

[7] BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen, Änderungsfassung vom 21.12.2023, https://intrapol.org/wp-content/uploads/2023/12/231221-Vergleichsversion-RefE-KRITIS-DachG.pdf, zuletzt abgerufen am 16.02.2024

[8] EU-Kommission, 2020, Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0829&from=EN, zuletzt abgerufen am 20.02.2024

[9] „Neue Leitlinie bestimmt Personal kritischer Infrastrukturen“, https://www.mags.nrw/pressemitteilung/neue-leitlinie-bestimmt-personal-kritischer-infrastrukturen, zuletzt abgerufen am 09.02.2024

[10] Petermann, T.; Bradke, H.; Lüllmann, A.; Poetzsch, M.; Riehm, U., 2010, Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung. Endbericht zum TA-Projekt, https://publikationen.bibliothek.kit.edu/1000103291, zuletzt abgerufen am 20.02.2024

[11] Schulze, K., Lorenz, D., Voss, M., Menschliches Verhalten bei Katastrophen, in: Schriftenreihe Sicherheit Nr. 22, Herausgegeben von Lars Gerhold, Roman Peperhove & Helga Jäckel, AG Interdisziplinäre Sicherheitsforschung, Forschungsforum Öffentliche Sicherheit, Freie Universität Berlin, Juni 2017

[12] Richter, D., 2023, Psychische Gesundheit während und nach der COVID-19-Krise, in: Sozialpsychiatrische Informationen, 53, 4

[12b] UBA, 2024, https://www.umweltbundesamt.de/daten/umwelt-gesundheit/gesundheitsrisiken-durch-hitze#indikatoren-der-lufttemperatur-heisse-tage-und-tropennachte, zuletzt abgerufen am 12.02.2024

[12c] BZgA (Bundeszentrale für gesundheitliche Aufklärung), ohne Datum, https://www.klima-mensch-gesundheit.de/hitzeschutz/babys-und-kinder/, zuletzt abgerufen am 12.02.2024

[12d] Deutsche Welle, 2023, https://www.dw.com/de/niedrigwasser-im-rhein-bremst-konjunktur/a-66155570, zuletzt abgerufen am 12.02.2024

[12e] Deutscher Bundestag, 2013, Bericht zur Risikoanalyse im Bevölkerungsschutz 2012, https://dserver.bundestag.de/btd/17/120/1712051.pdf, zuletzt abgerufen am 12.02.2024

[12f] Deutscher Bundestag, 2023, Bericht zur Risikoanalyse im Bevölkerungsschutz 2020 bis 2022, https://dserver.bundestag.de/btd/20/063/2006300.pdf, zuletzt abgerufen am 12.02.2024

[12g] BBK, 2007, Auswertungsbericht der dritten länderübergreifenden Krisenmanagementübung LÜKEX 2007,

Stellungnahme zum Fragenkatalog „KRITIS“ der Enquetekommission „Krisen- und Notfallmanagement“ (EK II – KRITIS – 01.03.2024)

https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/LUEKEX/luekex07-auswertungsbericht.pdf%3F__blob%3DpublicationFile%26v%3D7, zuletzt abgerufen am 12.02.2024

[13] BMI, 2009, Nationale Strategie zum Schutz kritischer Infrastrukturen, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 12.02.2024

[14] BMI, 2011, Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.html, zuletzt abgerufen am 12.02.2024

[14b] FwDV 100, 1999, https://lernkompass.idf.nrw/goto.php?target=file_793_download&client_id=Feuer, zuletzt abgerufen am 22.02.2024

[15] BMI, BMF, 2022, Bericht zur Hochwasserkatastrophe 2021: Katastrophenhilfe, Wiederaufbau und Evaluierungsprozesse, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2022/abschlussbericht-hochwasserkatastrophe.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 12.02.2024

[16] Klinger, I., Heckel, M., Shahda, S., Krisen, U., Stellmacher, S., Kurkowski, S., Junghanß, C., Ostgathe, C., 2022, COVID-19-Pandemiekrisenstäbe: Organisation, Befugnisse und Herausforderungen – Strukturelle Gegebenheiten verstehen und nutzen, Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz. 2022; 65(6): 650–657, doi: 10.1007/s00103-022-03542-x

[17] IM NRW, 2022, Katastrophenschutz der Zukunft - Abschlussbericht des vom Minister des Innern berufenen Kompetenzteams Katastrophenschutz, https://www.im.nrw/system/files/media/document/file/berkompetenzteam2_0.pdf, zuletzt abgerufen am 15.02.2024

[18] IM NRW, 2022, Vorlage 17/6531 vom 7. März 2022, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-6531.pdf, zuletzt abgerufen am 15.02.2024

[19] taz.de vom 23.12.2021, https://taz.de/Omikron-Variante-gefaehrdet-Versorgung/!5821243/, zuletzt abgerufen am 15.02.2024

[20] capital.de vom 05.01.2022, https://www.capital.de/wirtschaft-politik/feuerwehr-kliniken-polizei-so-bereitet-sich-die-kritische-infrastruktur-auf-omikron-vor, zuletzt abgerufen am 15.02.2024

[21] Berliner Morgenpost online vom 26.01.2022, https://www.morgenpost.de/vermischtes/article234408263/corona-deutsche-bahn-omikron-kritische-infrastruktur.html, zuletzt abgerufen am 15.02.2024

[22] wiwo.de vom 14.01.2022, https://www.wiwo.de/unternehmen/energie/kritische-infrastruktur-vor-der-omikron-welle-die-infizierten-schicht-koennte-das-gesamte-netz-steuern/27972614.html, zuletzt abgerufen am 15.02.2024

[23] IMK, 2024, Länderabgestimmten Stellungnahme des AK V „Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung“ der Ständigen Konferenz der Innenminister und -senatoren der Länder, 24.01.2024, liegt der Autorin vor

[24] Olofsson, A., 2011, Organizational crisis preparedness in heterogeneous societies: the OCPH model, Journal of Contingencies and Crisis Management, 19, 215-226. https://doi.org/10.1111/J.1468-5973.2011.00652.X

[25] Sandman, P. M., 1987, Risk communication: facing public outrage, EPA Journal, 2, 21–22, https://www.psandman.com/articles/facing.htm, zuletzt abgerufen am 20.02.2024

[26] Malecki, K., Keating, J., & Safdar, N., 2020, Crisis Communication and Public Perception of COVID-19 Risk in the Era of Social Media, Clinical Infectious Diseases: An Official Publication of the Infectious Diseases Society of America, 72, 697 - 702. https://doi.org/10.1093/cid/ciaa758

[27] BBK, 2023, Ergebnisse der Umfrage zum bundesweiten Warntag 2022, https://www.bbk.bund.de/SharedDocs/Downloads/DE/Warnung-Vorsorge/Umfrageergebnisse-BWT-2022.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 20.02.2024

[27b] https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Ausstattung-Gebrauchsgueter/Tabellen/a-evs-infotechnik-d.html, zuletzt abgerufen am 22.02.2024

[27c] https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/, zuletzt abgerufen am 22.02.2024

[28] Wikipedia, 2024, https://de.wikipedia.org/wiki/Falschinformationen_zur_COVID-19-Pandemie#Deutschland, zuletzt abgerufen am 20.02.2024

[29] Cook, J., Lewandowsky, S., & Ecker, U., 2017, Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence, PLoS ONE, 12. https://doi.org/10.1371/journal.pone.0175799

[30] BPB, 2019, Desinformation: Vom Kalten Krieg zum Informationszeitalter, https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290487/desinformation-vom-kalten-krieg-zum-informationszeitalter/, zuletzt abgerufen am 20.02.2024