LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/1290

A41

Zur Kritischen Infrastruktur des Landes Nordrhein-Westfalen

Dr. Frank Schnaack

21. Februar 2024

Inhaltsverzeichnis

Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen

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

Allgemein umfasst Kritische Infrastruktur Einrichtungen und Systeme, deren Beeinträchtigung erhebliche Auswirkungen auf die öffentliche Sicherheit, die wirtschaftliche Stabilität oder das öffentliche Wohlergehen hat. Sowohl staatliche als auch privatwirtschaftliche Einrichtungen können als Kritische Infrastruktur betrachtet werden.

1. Energieversorgung:
- Staatliche: Energieerzeugungsanlagen, Übertragungsnetze.
- Privat: Elektrizitätsversorger, Gasversorgungsunternehmen.

2. Wasserversorgung:
- Staatliche: Wasseraufbereitungsanlagen, Wasserreservoirs.
- Privat: Wasserversorgungsunternehmen.

3. Transportwesen:
- Staatliche: Flughäfen, Bahnhöfe, Verkehrsleitsysteme.
- Privat: Fluggesellschaften, Eisenbahngesellschaften.

4. Kommunikation:
- Staatliche: Telekommunikationsnetze, Rundfunkanstalten.
- Privat: Telekommunikationsunternehmen, Medienunternehmen.

5. Gesundheitswesen:
- Staatliche: Krankenhäuser, Gesundheitszentren.
- Privat: Medizinische Versorgungseinrichtungen, Pharmaunternehmen.

6. Finanzwesen:
- Staatliche: Zentralbanken, Finanzaufsichtsbehörden.
- Privat: Banken, Börsen.

7. IT-Infrastruktur:
- Staatliche: Regierungsnetzwerke, IT-Sicherheitsbehörden.
- Privat: Technologieunternehmen, Internetdienstanbieter.

8. Lebensmittelversorgung:
- Staatliche: Lebensmittelüberwachungseinrichtungen, Nahrungsmittelverarbeitungseinrichtungen.
- Privat: Lebensmittelproduzenten, Supermärkte.

Grundsätzlich sind die betroffenen Einzelbereiche der Infrastruktur in gegenseitiger Abhängigkeit zu betrachten. Somit geht es um übergreifende Sektoren, die, bei Einzelausfällen, Folgeausfälle aufweisen und somit die Gefahr als auch die Störungen potenzieren können. Ähnlich einem Dominoeffekt müssen die potenziellen Auswirkungen auf die Gesellschaft, im Falle einer Störung und der Fähigkeit, die Kontinuität der kritischen Dienstleistungen aufrechtzuerhalten, berücksichtigt werden.

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

Entsprechend den in der vorherigen Frage aufgezählten Bereichen werden nun Bereiche in der Gruppe „Pandemie“ und „Extremwetterereignisse“ erläutert:

Pandemien und Extremwetterereignisse können eine Vielzahl von Einrichtungen beeinflussen, insbesondere solche, die als Kritische Infrastruktur betrachtet werden.

A) Pandemien:

Die Weltgesundheitsorganisation (WHO) hat eine spezifische Definition für den Begriff Pandemie. Gemäß der WHO bedeutet eine Pandemie:

1. **Die Verbreitung:**
    - Eine Pandemie bezieht sich auf die weltweite Ausbreitung eines neuen Krankheitserregers, gegen den die Mehrheit der Menschen keine Immunität besitzt.

2. **Anhaltende Übertragung:**
    - Es muss eine anhaltende Übertragung der Krankheit von Mensch zu Mensch in mehreren Ländern oder Kontinenten stattfinden.

Ein Pandemieausbruch kann eine breite Palette von Krankheitsbildern umfassen, von milden bis zu schweren Krankheitsverläufen. Historisch bekannte Pandemien umfassen beispielsweise die Spanische Grippe von 1918, die H1N1-Influenza-Pandemie von 2009 und die COVID-19-Pandemie, die im Jahr 2019 durch das SARS-CoV-2-Virus ausgelöst wurde.

Der Begriff „Pandemie“ beschreibt das Ausmaß und die geografische Verbreitung einer Krankheit, nicht jedoch zwangsläufig die Schwere der Erkrankung. Eine Pandemie kann demnach auch eine relativ milde Krankheit betreffen, die sich geografisch ausbreitet.

1. Gesundheitswesen:
Krankenhäuser und Gesundheitseinrichtungen sind direkt von der Last der Behandlung von Kranken betroffen. Ein Mangel an Personal, medizinischer Ausrüstung und Arzneimitteln kann die Funktionsfähigkeit massiv beeinträchtigen.

2. Versorgungseinrichtungen:
Lebensmittelgeschäfte, Drogerien und Apotheken sind sicherlich primäre Bereiche. Der tägliche Bedarf könnte, aufgrund von Lieferkettenunterbrechungen, Schließungen oder einer höheren Nachfrage (Hamsterkäufe durch Panik), beeinträchtigt werden.

Aber auch **weitere Einrichtungen** des Versorgungsbereiches sind betroffen:

2.1. Bildungseinrichtung:
Sicherlich gehören Bildungseinrichtungen und Kindertagesstätten nicht zu der primär gefährdeten Einrichtung bei einer Pandemie. Diese sind eher als sekundär zu betrachten. Der Aufenthalt in einer Bildungseinrichtung sorgt für Austausch, sinnhafte Tätigkeit sowie Ablenkung vom Alltag.

Schulen, Hochschulen und Universitäten sind wichtig für die Ausbildung der Bevölkerung. In Krisensituationen können sie jedoch geschlossen werden oder ihre Funktionsweise beeinträchtigt sein. Dies führt dann zu einer gesellschaftlichen Isolation von Schülern, Studenten, aber auch Lehrern und Hochschuldozenten. Hier kann sicherlich mit der IT, sofern diese Infrastruktur nicht geschädigt wurde, kurzfristiger Ersatz geschaffen werden

(Zoom, GoTo-Webinar, Online-Vorlesungen, Online-Unterricht). Hier ist jedoch anzumerken, dass es immer noch Familien gibt, die die Voraussetzungen für einen digitalen Eintritt in die Lernwelt mangels finanzieller Mittel nicht erfüllen können.

Wenn Kinder und Jugendliche über einen längeren Zeitraum zu Hause bleiben müssen, sorgt steigender Stress, aufgrund des „Nichtstuns“ und der Unterforderung/Langeweile, für erhöhtes Konfliktpotential in der Familie.

2.2. Regierungsbehörden:
Verwaltungen, Polizei, Feuerwehr und andere öffentliche Dienste sind entscheidend für die Aufrechterhaltung der Infrastruktur sowie den Schutz der Bevölkerung in Notfällen. Kommen diese auch nur teilweise zum Erliegen, ist bereits dann die Sicherheit und der Schutz der Bevölkerung gefährdet.

2.3. Soziale Dienste:
Einrichtungen, die Sozialdienste anbieten (Unterstützung von Personen im häuslichen Umfeld oder Obdachlosenbetreuung), könnten im Rahmen einer Pandemie ihre Dienstleistungen nicht mehr ausüben. Somit wären diese Personen auf sich selbst gestellt. Da diese Personen hierzu, entweder aus gesundheitlichen oder psychischen Gründen, nicht in der Lage sind, gehören sie zu der Gruppe der lebensbedrohlich Gefährdeten (keine Selbstversorgung möglich).

2.4. Finanzdienstleistungen:
Banken und andere Finanzinstitute spielen eine entscheidende Rolle bei der Bereitstellung von finanziellen Ressourcen, Zahlungsdiensten und wirtschaftlicher Stabilität. Müssen diese wegen einer Pandemie schließen oder bieten nur noch eingeschränkte Service-Dienste an, so werden Bargeldabhebungen, aber auch Schaltergeschäfte stark eingeschränkt. Dies trifft gerade ältere Menschen, welche sich lieber ihrem Bankberater anvertrauen und sich mit den elektronischen Geräten wenig oder kaum auskennen. Auch ist im Falle einer Transporteinschränkung bei der Pandemie die Versorgung mit Bargeld an den Geldautomaten nicht mehr ausreichend gegeben. Somit müssen die Kunden auf Karten-zahlung umsteigen – sofern die IT-Infrastruktur funktioniert.

2.5. Logistik und Versorgungsketten:
Logistik und Versorgung von Gütern sind während einer Pandemie wichtig, um die kontinuierliche Versorgung mit Lebensmitteln, Medikamenten und anderen wesentlichen Gütern sicherzustellen.

2.4. Sicherheitsdienste:
Private Sicherheitsunternehmen und Sicherheitsinfrastrukturen sind wichtig, um den Schutz von Einrichtungen, Unternehmen und der Bevölkerung zu gewährleisten.

2.5. Technologie und Informationsdienste:
Internetdienstanbieter und andere Technologieeinrichtungen sind entscheidend für die Aufrechterhaltung der Kommunikation und den Informationszugang. Hier muss während einer Pandemie die Aufrechterhaltung sichergestellt werden.

2.6. Landwirtschaft und Nahrungsmittelproduktion:
Landwirtschaftliche Betriebe, Lebensmittelverarbeitungsanlagen müssen in der Pandemie weiter aufrechterhalten werden. Geschieht dies nicht, wird eine Weiterversorgung mit Produkten schwierig bis unmöglich, da die Herstellung von Lebensmitteln nicht mehr gewährleistet ist. Darüber hinaus müssen Betriebe mit Tierhaltung ihre täglichen Arbeiten verrichten (Melken, Fütterung, etc.), da sonst die Tiere Schaden nehmen.

2.7. Energieunternehmen:
Neben der Energieerzeugung sind auch Dienstleistungen wie Strom- und Gasversorgung für Haushalte und Unternehmen entscheidend. Im Falle eines Ausfalles muss Service-Personal vor Ort arbeiten können. Schließlich sind der Schutz und die Aufrechterhaltung ihrer Funktionsfähigkeit entscheidend für das Wohlbefinden und die Sicherheit der Bevölkerung (ohne Stromversorgung kein Kochen, keine Wärmepumpe, kein heißes Wasser usw.).

3. Kommunikation:
Die verstärkte Nutzung von Kommunikationsnetzen (Smartphones, Videotelefonie, Telefonie über VoIP), insbesondere von Internetnutzung durch Home-Office, Fernunterricht, aber auch Streaming von Unterhaltungsprogrammen mit erhöhtem Datentransfer, kann zu Überlastungen des Netzsystems führen. Gleichzeitig sind Kommunikationsdienste entscheidend für die Verbreitung von Informationen im Zusammenhang mit der Pandemie.

B) Extremwetterereignisse:

Auch wenn einige Aspekte bereits beim Pandemie-Kapitel Erwähnung fanden, werden sie in diesem Kapitel mit aufgeführt, da sie auch die Extremwetterereignisse betreffen.

Extremwetterereignisse werden als Wetterereignisse definiert, die ungewöhnlich intensiv oder ungewöhnlich im Vergleich zu den durchschnittlichen Wetterbedingungen in einem bestimmten Gebiet sind. Diese Ereignisse können verschiedene Formen annehmen, einschließlich extrem hoher oder niedriger Temperaturen, starker Niederschläge, intensiver Stürme, Dürren, Überschwemmungen, Wirbelstürme und anderer meteorologischer Phänomene. Im Allgemeinen bezieht sich der Begriff auf Wetterereignisse, die signifikante Auswirkungen auf die Umwelt, die Gesellschaft und die Wirtschaft haben.

1. Energieversorgung:
Stürme, Überschwemmungen oder extreme Hitze können die Energieinfrastruktur beeinträchtigen, einschließlich Stromnetze, Kraftwerke und Kraftstofflager.

Hier können Kurzschlüsse durch Wassereinbruch entstehen oder Ausfälle des Kühlungssystems durch großen Hitzeeinfluss. Stürme können zu Schäden an Masten und Kabeln führen, sodass eine Energieversorgung nicht mehr gewährleistet ist. Auch sind Erdrutsche bei Starkregen und Sturm möglich. Durch die Erdverschiebung kann es zum Freilegen der Versorgungsleitungen mit anschließendem Kurzschluss durch Wassereinbruch kommen oder sogar zum Abriss der Leitungen kommen. Hinzu kommt noch, dass die Leitungen unpassierbar werden, sodass eine Instandsetzung in der Akutsituation extrem erschwert wird oder nicht möglich ist.

2. Transportwesen:
Straßen, Brücken können durch extreme Wetterereignisse beschädigt oder unpassierbar werden, was die Mobilität erschwert oder zum Erliegen bringt. Auch das Schienensystem kann durch Unterspülung, Überschwemmung unpassierbar werden. Auch bei großer Hitze kann es hier zu Funktionsausfällen kommen, sodass defekte Weichen und defekte Signale eine Versorgung auf der Schiene erschweren bis unmöglich machen.

3. Wasserversorgung:
Überschwemmungen oder Dürren können die Wasserversorgung beeinträchtigen, indem sie Wasseraufbereitungsanlagen schädigen oder den Zugang zu Wasserquellen erschweren. Bei langanhaltendem Regen können die Talsperren überfüllt werden, sodass Wasser abgelassen werden muss, um Dammbrüche zu vermeiden. Kommt neben dem bereits vorhandenen Hochwasser noch das abgelassene Wasser der Talsperren hinzu, so drohen katastrophale Überschwemmungen.

Bei einer Dürre ist gerade die ländliche Wasserversorgung für Agrarwirtschaft und Viehzucht bedroht. Felder können nicht ausreichend bewässert werden, sodass Pflanzen (Getreide, Obst, Gemüse) eingehen. Auch werden die Löschteiche in Wald- und Landgebieten nicht mehr ausreichend Wasser aufweisen, um im Notfall mit dem dort vorhandenen Wasser Brände zu löschen.

4. Gesundheitswesen:
Krankenhäuser und medizinische Einrichtungen können auch durch Extremwetterereignisse schwer beschädigt werden, was zu einer Verringerung der verfügbaren Kapazitäten von medizinischer Versorgung führt (Beispiele: Keller unter Wasser; Wasserschäden in Gebäuden; überhitzte Stationen ohne Klimaanlagen, Temperatur steht bei bis zu 32°C in den Zimmern und Fluren).

5. Lebensmittelversorgung:
Ernteausfälle, Transportunterbrechungen und Schäden an Lagerhäusern können die Verfügbarkeit von Lebensmitteln beeinträchtigen. Der Ausfall von Kühlanlagen – und somit ein Unterbrechen der Kühlkette – kann zum Verderben von Lebensmitteln führen.

6. Kommunikation:
Extremwetterereignisse können Kommunikationsinfrastrukturen beeinträchtigen oder vollständig zerstören, indem sie Mobilfunkmasten beschädigen oder den Zugang zu Breitbanddiensten stören oder sogar unmöglich machen. IT-Ausfälle durch Hitze und Wasser sind möglich.

Fazit:
Sowohl bei Pandemien als auch bei Extremwetterereignissen sind die Resilienz und Anpassungsfähigkeit der Kritischen Infrastrukturen entscheidend, um den Betrieb aufrechtzuerhalten und sich auf unvorhergesehene Herausforderungen einzustellen. Entsprechende Pläne zur Notfallvorsorge und -reaktion sind zu entwickeln, um die Auswirkungen auf Kritische Infrastrukturen zu minimieren. Komplett beseitigen lassen sich Schäden der KRITIS durch Vorsorge NICHT. Da hier ein Zusammenspiel aller Bereiche der Infrastruktur vorhanden ist, ähnlich dem Zusammenspiel der Zahnräder in einer mechanischen Uhr, sorgt der Ausfall eines Bereiches auch für Einschränkungen der anderen Bereiche. Somit ist die KRITIS grundsätzlich als Ganzes zu betrachten und muss auch bestmöglich als Ganzes geschützt werden.

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

In Nordrhein-Westfalen (NRW) gibt es verschiedene Gesetze und Verordnungen, die sich mit Kritischer Infrastruktur befassen:

1. BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik):

Das BSI-Gesetz regelt die Aufgaben und Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik. Es enthält Bestimmungen zur Sicherheit von informationstechnischen Systemen, die in den Kritischen Infrastrukturen eine wichtige Rolle spielen.

2. IT-Sicherheitsgesetz:
Das IT-Sicherheitsgesetz regelt die Sicherheit von informationstechnischen Systemen und Kritischen Infrastrukturen. Es verpflichtet Betreiber Kritischer Infrastrukturen, angemessene Maßnahmen zur Gewährleistung der IT-Sicherheit zu ergreifen und bestimmte Sicherheitsvorfälle zu melden.

Besonderer Augenmerk ist auf die §§ 8a bis 8i des BSI-Gesetzes zu richten. Hier werden die Sicherheitsmaßnahmen für Betreiber einer Kritischen Infrastruktur und die Zusammenarbeit zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und deren Betreibern geregelt.

§ 8a - Schutzbedarf und Mindeststandards:
Legt den Schutzbedarf von informationstechnischen Systemen und Netzen fest, die für die Funktionsfähigkeit der Kritischen Infrastrukturen wesentlich sind. Zudem werden Mindeststandards für die Informationssicherheit definiert.

§ 8b - Meldung erheblicher IT-Sicherheitsvorfälle:
Betreiber Kritischer Infrastrukturen sind verpflichtet, erhebliche IT-Sicherheitsvorfälle dem BSI zu melden. Dieser Paragraph regelt die Meldepflicht und den Umgang mit den Meldungen.

§ 8c - Verpflichtung zur Umsetzung von Maßnahmen:
Betreiber sind verpflichtet, angemessene organisatorische und technische Maßnahmen zur Gewährleistung der IT-Sicherheit zu treffen. Dieser Paragraph legt die Einzelheiten dazu fest.

§ 8d - Audits:
Das BSI hat das Recht, Audits bei den Betreibern Kritischer Infrastrukturen durchzuführen, um die Umsetzung der Sicherheitsmaßnahmen zu überprüfen.

§ 8e - Information und Zusammenarbeit:
Das BSI ist zu informieren und mit diesem muss zusammengearbeitet werden, ➔ im Hinblick auf die IT-Sicherheit.

§ 8f - Durchführung von Sicherheitsüberprüfungen:
Das BSI kann Sicherheitsüberprüfungen bei Betreibern Kritischer Infrastrukturen durchführen, um die Einhaltung der Sicherheitsvorschriften zu überprüfen.

§ 8g - Anordnung zur Einhaltung von Maßnahmen:
Falls ein Betreiber Kritischer Infrastrukturen seinen Pflichten nicht nachkommt, kann das BSI Anordnungen zur Einhaltung der erforderlichen Maßnahmen erlassen.

§ 8h - Auskunftspflichten und Bußgeldvorschriften:
Dieser Paragraph regelt Auskunftspflichten gegenüber dem BSI und enthält Bußgeldvorschriften für Verstöße gegen die Sicherheitsbestimmungen.

§ 8i - Anwendung des Verwaltungsverfahrensgesetzes:
Für die Anwendung des Verwaltungsverfahrensgesetzes gelten spezielle Regelungen im Zusammenhang mit den in den vorherigen Paragraphen festgelegten Maßnahmen.

3. Kritisverordnung (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz):
Die Kritisverordnung konkretisiert, welche Sektoren und Unternehmen als Kritische Infrastruktur gelten. Sie enthält Regelungen zu den Mindestanforderungen an die IT-Sicherheit und die Meldung von Sicherheitsvorfällen.

Auszug:
§ 8 Absatz 1 Satz 1 des BSI-Gesetzes:

"Das Bundesamt für Sicherheit in der Informationstechnik trifft Maßnahmen zur Abwehr von Gefahren für die Sicherheit der informationstechnischen Systeme, insbesondere durch die Entwicklung von Sicherheitsstandards und durch die Zulassung von Produkten sowie durch

Maßnahmen zur frühzeitigen Erkennung und Abwehr von Sicherheitsgefahren bei informationstechnischen Systemen."

Die Nummern 2 bis 4, auf die sich der Abschnitt des §8 Absatz 1 des BSIG bezieht, sind im Detail wie folgt:

- **Nummer 2**: Maßnahmen zur Erhöhung der Sicherheit von informationstechnischen Systemen bei der Verarbeitung, Nutzung und Speicherung von Informationen;
- **Nummer 3**: Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und informationstechnischen Systemen;
- **Nummer 4:** Maßnahmen zur Gewährleistung der Funktionsfähigkeit der informationstechnischen Systeme.

4. Katastrophenschutzgesetz (KatSG NRW):
Auf Landesebene in Nordrhein-Westfalen gibt es das Katastrophenschutzgesetz, das Maßnahmen zur Vorsorge, zur Bewältigung von Katastrophen und zur Zusammenarbeit aller beteiligten Stellen regelt. Siehe auch: Ministerium für Inneres und Kommunales in NRW.

5. Gesetz über den Zivilschutz und die Katastrophenhilfe (ZSKG):
Das Zivilschutz- und Katastrophenhilfegesetz ist auf Bundesebene relevant und regelt unter anderem den Schutz der Bevölkerung und den Einsatz von Streitkräften im Katastrophenfall.

Die Umsetzung der Anforderungen an Kritische Infrastrukturen erfolgt in NRW in erster Linie durch die bundesrechtlichen Regelungen, insbesondere durch die Kritisverordnung des Bundes.

Föderalistischen Strukturen:
Zuständigkeiten und Kompetenzen sind zwischen dem Bund und den einzelnen Bundesländern aufgeteilt sind (Bundes-/Landeskatastrophenschutz, THW, HiOrgs, Feuerwehren, Bundeswehr, Landes-/Bundespolizei, Straßenmeistereien etc.). Wenn es um Kritische Infrastrukturen (KRITIS) geht, spielen sowohl der Bund als auch die Länder eine Rolle.

Die föderalistischen Strukturen können im Rahmen der KRITIS wie folgt unterteilt werden:

1. Bundesebene:
Der Bund in Deutschland erlässt bundeseinheitliche Regelungen, die für das gesamte Land gelten. Das Bundesministerium des Innern, für Bau und Heimat (BMI) ist maßgeblich für die Regelungen im Bereich KRITIS zuständig. Die Kritisverordnung auf Bundesebene (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) definiert, welche Sektoren als Kritische Infrastrukturen gelten und enthält Mindestanforderungen, z. B. an die IT-Sicherheit.

2. Landesebene:
Die Bundesländer, hier Nordrhein-Westfalen (NRW), haben die Möglichkeit, bestimmte bundesrechtliche Regelungen zu konkretisieren oder zu erweitern. Dies geschieht durch eigene Landesverordnungen oder Erlasse. Auf Landesebene sind in der Regel das Innenministerium oder vergleichbare Ressorts für die Umsetzung und Überwachung der Maßnahmen im Bereich KRITIS zuständig.

3. Zusammenarbeit:
Es besteht eine enge Zusammenarbeit zwischen Bund und Land im Bereich KRITIS. Während der Bund bundeseinheitliche Standards und Rahmenvorgaben festlegt, kann NRW zusätzliche Maßnahmen ergreifen, die den spezifischen Bedürfnissen und Gegebenheiten vor Ort gerecht werden.

Die föderale Struktur ermöglicht eine gewisse Flexibilität und Anpassungsfähigkeit, um regionale Besonderheiten zu berücksichtigen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Bundesebene spielt ebenfalls eine Schlüsselrolle bei der Beratung und Unterstützung der Länder und Betreiber Kritischer Infrastrukturen. Es koordiniert nationale Cyberabwehrmaßnahmen und bietet Leitlinien zur Umsetzung von IT-Sicherheitsmaßnahmen.

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

Im Rahmen der föderalen Strukturen in Deutschland sind verschiedene Gremien, sowohl auf Bundesebene als auch auf Landesebene, für die Sicherheit Kritischer Infrastrukturen (KRITIS) zuständig. Hier sind die wichtigsten und deren Zuständigkeiten:

A) Bundesebene:

1. Bundesministerium des Innern, für Bau und Heimat (BMI):
Das BMI ist maßgeblich für die gesetzlichen Grundlagen und Rahmenbedingungen im Bereich KRITIS verantwortlich. Es erlässt bundeseinheitliche Regelungen wie beispielsweise die Kritisverordnung.

2. Bundesamt für Sicherheit in der Informationstechnik (BSI):
Das BSI ist eine zentrale Instanz auf Bundesebene und spielt eine Schlüsselrolle bei der Sicherheit von informationstechnischen Systemen. Es erlässt technische Richtlinien und Empfehlungen, berät die Länder und Betreiber Kritischer Infrastrukturen und koordiniert nationale Cyberabwehrmaßnahmen.

3. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK):
Das BBK unterstützt Bund und Länder in Fragen des Zivilschutzes und der Katastrophenhilfe. Es kann bei der Planung und Bewältigung von Krisen und Katastrophen involviert sein, einschließlich solcher, die Kritische Infrastrukturen betreffen.

B) Landesebene NRW:

1. Innenministerium des Landes:
Das Innenministerium des Landes ist in der Regel zuständig für die Umsetzung der bundeseinheitlichen Regelungen auf Landesebene. Es erlässt eigene Verordnungen oder verabschiedet Erlasse, um die spezifischen Gegebenheiten des Landes zu berücksichtigen.

2. Landesamt für Sicherheit in der Informationstechnik (LSI) oder vergleichbare Einrichtungen:
Das Landesamt für Sicherheit in der Informationstechnik (LSI) ist für die Umsetzung und Überwachung von IT-Sicherheitsmaßnahmen innerhalb des Landes verantwortlich. Es ist eine Einrichtung, die dem Ministerium für Inneres des Landes Nordrhein-Westfalen unterstellt ist. Dieses berät und unterstützt Landesbehörden, Kommunen sowie Betreiber kritischer Infrastrukturen in Nordrhein-Westfalen in Fragen der Informationssicherheit (Analyse und Bewältigung von Sicherheitsvorfällen im Bereich der Informationstechnik). Ferner analysiert das Amt aktuelle Bedrohungslagen im Bereich der Informationssicherheit und gibt Frühwarnungen heraus, um auf potenzielle Risiken und Gefahren aufmerksam zu machen. Es entwickelt und fördert Sicherheitsstandards und -maßnahmen für die Informationstechnik und ist in der Sensibilisierung und Schulung von Behörden, Unternehmen und der Bevölkerung für das Thema IT-Sicherheit aktiv.

3. weitere zuständige Behörden und Stellen:
Je nach Land können verschiedene Behörden und Stellen für die Umsetzung der Maßnahmen im Bereich KRITIS zuständig sein. Dies wären Polizei, Feuerwehr und andere relevante Behörden des Katastrophenschutzes.

Die Zusammenarbeit zwischen Bund und Ländern ist für den Austausch von Informationen und die Koordination von Maßnahmen entscheidend. Die föderalen Strukturen ermöglichen eine flexible und angepasste Herangehensweise an die Sicherheit Kritischer Infrastrukturen mit Fokus auf die jeweils regionalen Gegebenheiten.

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

Ich möchte hier eher erwähnen, was häufig vernachlässigt wird bzw. was eher einer freiwilligen Maßnahme unterliegt. Die Frage ist, ob hier die freiwilligen Maßnahmen nachhaltig umgesetzt werden oder der Gesetzgeber durch Erlasse und Verordnungen höhere Sicherheit für die Bevölkerung erreicht. Natürlich ist in der Privatwirtschaft jegliche gesetzliche Regulierung von Seiten der Betreiber mit personellem Mehraufwand, aber auch mit Kosten in den Bereichen Human Resource Management, Logistik und Material möglich. Gerade wenn es um Anschaffungen im Sinne der Sicherheit geht, muss eruiert werden, wo Zuschüsse durch die Landesregierung notwendig sind oder sogar die Kosten durch das Land NRW vollständig übernommen werden. Es ist zu bedenken, dass Investitionen für Präventivmaßnahmen, auch wenn sie anfangs hoch erscheinen, eine gute Investition sind um die evtl. Ereigniskosten (Schäden für Infrastruktur, Menschenleben) zu verringern.

Natürlich ist bei Investitionen in die KRITIS niemals ein „Return on Invest“ wie in der freien Wirtschaft garantiert. Hier kann nur vermutet werden, wie viel Folgekosten bei Ereignissen vermieden werden könnten und wie viel Menschenleben gerettet werden. Eine Sicherheit oder Gewährleistung gibt es im Rahmen der KRITIS-Investition nicht.

Zu bedenken ist auch, dass eine gesetzliche Überregulierung Unternehmen, aber auch den Behörden, mehr Stolpersteine bei der Umsetzung in den Weg legt. Je enger der gesetzliche Rahmen, desto schwieriger ist der individuelle Handlungsrahmen vor Ort. Hier muss auch Job-Enrichment[1] und Job-Enlargement[2] während der Krise berücksichtigt werden. Eine Überregulierung durch Gesetze kann zu Überforderung der Mitarbeiter vor Ort führen und die Bewältigung von Krisen erschweren.

Weitere Einrichtungen die unserer Aufmerksamkeit bedürfen:
Die öffentliche Wasserversorgung und Abwasserbeseitigung sowie seit kurzem auch die Siedlungsabfallentsorgung werden in Deutschland zu den Kritischen Infrastrukturen gezählt.

„Der Schutz der Kritischen Infrastrukturen wird jedoch als gemeinsame Aufgabe von Staat, Wirtschaft und Öffentlichkeit erkannt, sodass auch weitere staatliche Stellen auf allen Ebenen, die Betreiber der Kritischen Infrastrukturen und ihre Verbände, die Wissenschaft und Forschung und nicht zuletzt auch die Bevölkerung angesprochen werden. Besondere Bedeutung wird vor allem einer vertrauensvollen und konstruktiven Zusammenarbeit zwischen den staatlichen Stellen und den vorwiegend privatwirtschaftlich organisierten Betreibern beigemessen. Freiwilligen Selbstverpflichtungen der Wirtschaft wird daher grundsätzlich Vorrang vor gesetzlichen Regelungen eingeräumt (BMI 2009, S.2). Entsprechend

[1] Erläuterung zu „Job-Enrichment“: Maßnahme der Arbeitsgestaltung. Dabei werden dem Arbeitnehmer anspruchsvollere Aufgaben zugewiesen und ein höheres Maß an Entscheidungsfreiheit gewährt.
[2] Erläuterung zu „Job-Enlargement“: Sieht vor, dass der betreffende Mitarbeiter seinen Aufgabenbereich erweitert. Dabei handelt sich um zusätzliche Aufgaben auf dem gleichen Anforderungsniveau.

existiert in Deutschland auch kein übergreifendes Gesetz für den Schutz der Kritischen Infrastrukturen, obschon im Laufe der Zeit einzelne Aspekte in Fachgesetzen geregelt wurden.
Die Ausgestaltung der Zusammenarbeit zwischen staatlichen und privaten Akteuren wird in der KRITIS-Strategie nur skizziert. Als wesentliche Arbeitspakete werden die Festlegung allgemeiner Schutzziele, die Analyse und Bewertung von Gefährdungen, die Festlegung und Umsetzung von Schutzmaßnahmen (in erster Linie durch Verbands-lösungen, interne Regelwerke oder unternehmenseigene Schutzkonzepte) sowie ein kontinuierlicher Risikokommunikationsprozess genannt. Zur Umsetzung dieser Schritte sollen institutionalisierte Plattformen zwischen Staat, Behörden, Unternehmen und Verbänden organisiert werden (BMI 2009, S. 14 f.)."

Dies war der Stand der Bundesregierung im Oktober 2023. Zitiert aus Drucksache 20/8888 vom 23.10.2023, Deutscher Bundestag, 20. Wahlperiode.

„Dem Ansatz der freiwilligen Selbstverpflichtung der KRITIS-Strategie folgend sollen gesetzliche Regelungen nur dann greifen, wenn erhebliche festgestellte Sicherheitsmängel auf freiwilliger Basis nicht beseitigt werden bzw. bestehende gesetzliche Regelungen aufgrund neuer Gefahren und Risiken nicht ausreichenden Schutz bieten (BMI 2009, S. 12 f.). Dies und die Notwendigkeit, Vorgaben von europäischer Ebene in deutsches Recht zu überführen, haben im Laufe der Zeit dazu geführt, dass einzelne Aspekte des Schutzes Kritischer Infrastrukturen in Fachgesetzen festgeschrieben wurden.
Der Schutz der Informationssicherheit nimmt in diesem Kontext eine besondere Rolle ein. Die Prüfung regulatorischer Instrumente in diesem Bereich wurde erstmals im Rahmen der „Cyber-Sicherheitsstrategie für Deutschland", die 2011 den NPSI von 2005 ablöste, in Erwägung gezogen. Angesichts der wachsenden Bedrohung wurden in der Cyber-Sicherheitsstrategie Maßnahmen zur Stärkung der IT-Sicherheit erörtert, so im Bereich der Kritischen Informationsinfrastrukturen beispielsweise die Prüfung von rechtlichen Verpflichtungen zur stärkeren Verzahnung von Staat und Wirtschaft oder von gesetzlichen Vorgaben in Bezug auf Schutzmaßnahmen (BMI 2011a, S. 6 f.). Auch das BSI gelangte zur Einschätzung, dass der rein freiwillige Ansatz im Rahmen der öffentlich-privaten Kooperation UP KRITIS nicht ausreichend sei, um ein angemessenes IT-Sicherheitsniveau in allen KRITIS-Sektoren zu erreichen. So engagierten sich gemäß dem BSI (2015a, S. 41 ff.) nicht alle KRITIS-Sektoren im gleichen Maße im UP KRITIS und auch bei den Betreibern zeigten sich große Unterschiede hinsichtlich der Umsetzung von Schutzmaßnahmen. Diese Überlegungen und Feststellungen mündeten 2015 schließlich in das IT-Sicherheitsgesetz (Art. 1), durch das gesetzliche Regelungen zur Erhöhung der Informationssicherheit auch in Kritischen Infrastrukturen eingeführt wurden. Seitdem sind die Betreiber von Kritischen Infrastrukturen verpflichtet, bei IT-Systemen, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, ein Mindestmaß an Informationssicherheit einzuhalten und dies gegenüber dem BSI auch regelmäßig nachzuweisen." (Auszug: Drucksache 20/8888 des Deutschen Bundestags, ebenda)

Es gibt **neun Sektoren** (dazu zählen außerdem Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Finanz- und Versicherungswesen, Staat und Verwaltung, Medien und Kultur). Diese wurden auf Bundesebene **in 29 Branchen** weiter differenziert, so z. B. der Sektor Wasser in die öffentliche Wasserversorgung und die öffentliche Abwasserbeseitigung (siehe dazu auch Abbildung 1 auf der folgenden Seite).

Im Gegensatz zur Definition von Bund und Ländern jedoch handelt es sich gemäß BSIG bei den Kritischen Infrastrukturen nicht um ganze Sektoren bzw. alle dazugehörigen Organisationen, sondern nur um einzelne Einrichtungen oder Anlagen in diesen Sektoren, die kritische Dienstleistungen erbringen, also Dienstleistungen, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen für die öffentliche Sicherheit führen würden. Ob Einrichtungen oder Anlagen solche kritischen Dienstleistungen erbringen, ist vom Erreichen oder Überschreiten von Schwellenwerten abhängig. Die Höhe

dieser Schwellenwerte ist für die verschiedenen Anlagenkategorien, die kritische Dienstleistungen erbringen, in der BSI-Kritisverordnung (BSI-KritisV) festgelegt.
2021 wurde im Rahmen der Novellierung des BSIG durch das zweite IT-Sicherheitsgesetz (Art. 1) mit der Siedlungsabfallentsorgung schließlich ein neuer KRITIS-Sektor hinzugefügt.[3]

Auch sollen mit dem KRITIS-Dachgesetz die Vorgaben der Richtlinie (EU) 2022/255717 in nationales Recht umgesetzt werden.[4]

Abbildung 1:[5]

Sektoreneinteilung gemäß Bund und Länder	Sektoreneinteilung gemäß BSIG
Energie	Energie
Ernährung	Ernährung
Finanz- und Versicherungswirtschaft	Finanz- und Versicherungswesen
Gesundheit	Gesundheit
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation
Medien und Kultur	
	Siedlungsabfallentsorgung
Staat und Verwaltung	
Transport und Verkehr	Transport und Verkehr
Wasser	Wasser

Die Siedlungsabfallentsorgung – und damit die Abfallwirtschaft – ist als kritischer Sektor ein relevanter Teil der staatlichen Daseinsvorsorge. Insbesondere die Kommunen stehen vor der Aufgabe, die Entsorgung von Siedlungsabfällen, also die Sammlung, Beseitigung und Verwertung der Abfälle, zu gewährleisten und die Sicherheit der dazugehörigen IT-Infrastrukturen der Siedlungsabfallentsorgung zu schützen. Welche Ziele, Aufgaben und Herausforderungen damit einhergehen, wird im Folgenden aufgeführt.

„Grundsätzlich unterliegen Abfälle in Europa der Warenverkehrs- und Wettbewerbsfreiheit. Nach den in Artikel 16 Abs. 1 der Richtline 2008/98/EG19 (Abfallrahmenrichtlinie) formulierten Grundsätzen der Entsorgungsautarkie und der Nähe für gemischte Siedlungsabfälle aus privaten Haushalten soll aber jeder Mitgliedstaat dafür Sorge tragen, dass ein integriertes und angemessenes Netz von Anlagen zur Verwertung und Beseitigung von Siedlungsabfällen errichtet wird. Artikel 4 der Abfallrahmenrichtlinie legt auch fest, wie Abfälle erfasst und entsorgt werden sollen. Die Basis für diese Regelungen bildet die Abfallhierarchie […]. Die Vorgaben der Abfallrahmenrichtlinie werden durch das KrWG ins deutsche Recht umgesetzt. Abfälle im Sinne des § 3 KrWG sind alle Stoffe oder Gegenstände, derer sich ihr Besitzer entledigt, entledigen will oder entledigen muss. Das KrWG regelt u. a., welche Abfälle dem örE [öffentlich-rechtlichen Entsorgungsträger] zu überlassen sind und welche nicht.

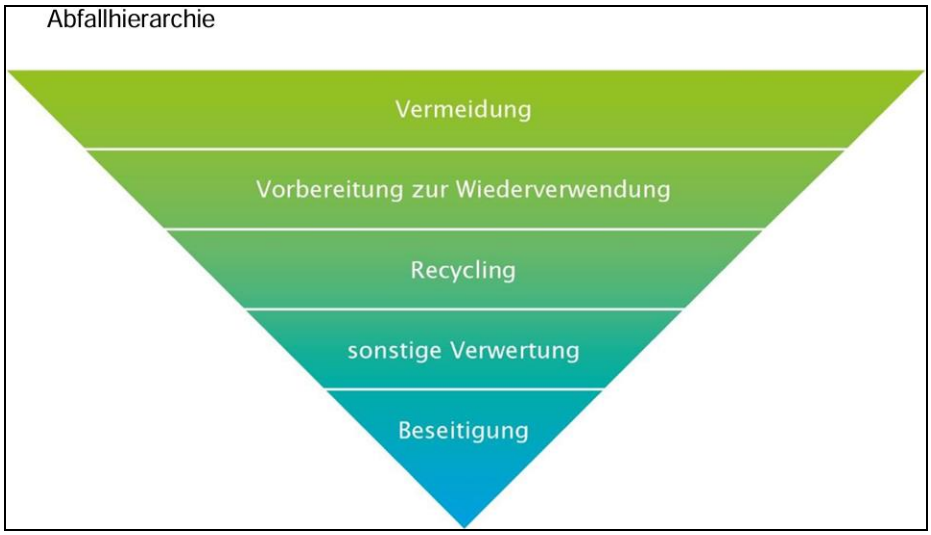
[3] Vgl. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.5.2021: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig_2-0.html#:~:text=Durch%20die%20Unterzeichnung%20des%20Bundespr%C3%A4sidenten,Mai%202021%20gebilligt

[4] Vgl. Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

[5] Siehe Quelle: nach BBK 2020, S. 24, und § 2 Abs. 10 Nr. 1 BSIG (23.6.2021); https://www.bundestag.de/resource/%20blob/978336/f75892c69427c2ea941cdf13fe535f01/20_8888.pdf

Öffentlich-rechtliche Entsorgungsträger – in der Regel Landkreise und kreisfreie Städte – sind grundsätzlich für die Entsorgung aller in ihrem Gebiet anfallenden Siedlungsabfälle zuständig. Dabei handelt es sich um Abfälle aus privaten Haushaltungen, die nicht in eigenen Anlagen verwertet werden (§ 17 u. § 20 KrWG). Abfälle sind zu verwerten oder, falls eine Verwertung nicht möglich ist, zu beseitigen. Grundsätzlich gilt, dass Abfälle zur Beseitigung in Deutschland nur deponiert werden dürfen, wenn zuvor verwertbare Bestandteile abgetrennt und der organische Anteil reduziert wurden (§ 6 Deponie-verordnung).“[6]

Abbildung 2:[7]



Für die Vorbereitung zur Wiederverwendung und das Recycling von Siedlungsabfällen legt § 14 KrWG quantitative Ziele fest. Sofern es für die Vorbereitung zur Wiederverwendung, das Recycling oder andere Verwertungsverfahren erforderlich ist, sind Abfälle nach Art und Beschaffenheit getrennt zu erfassen und zu behandeln (§ 9 KrWG).[8] [9]

„Grundsätzlich lassen sich zwei verschiedene Systeme unterscheiden: das Hol- und das Bringsystem. Im Holsystem werden die Abfallsammelbehältnisse oder Einzelstücke (sperrige Abfälle, Elektroaltgeräte) unmittelbar am Anfallort bereitgestellt. Die befüllten Behältnisse werden dann von den Abfallerzeugern oder dem Entsorgungsteam zur Entleerung/Abfuhr an den nächstgelegenen Straßenrand gebracht, wo sie von Sammelfahrzeugen abgefahren werden. Das Holsystem kommt üblicherweise bei folgenden Abfallarten zum Einsatz:

- Abfälle, die regelmäßig mit hohem Aufkommen anfallen (Restabfall, Bioabfall, Leichtverpackungen sowie PPK);
- Abfälle, die spezieller Aufmerksamkeit bedürfen (Restabfall und Bioabfall);
- Abfälle, die von einem Großteil der Bevölkerung nicht selbst transportiert werden können (sperrige Abfälle, Elektroaltgeräte).“[10]

---

[6] Drucksache 20/8888, Deutscher Bundestag, 23.10.2023 (Bericht: Technikfolgenabschätzung – Chancen und Risiken der Digitalisierung kritischer kommunaler Infrastrukturen an den Beispielen der Wasser- und Abfallwirtschaft):
https://www.bundestag.de/resource/blob/978336/f75892c69427c2ea941cdf13fe535f01/20_8888.pdf

[7] Quelle: nach VDI ZRE o. J.

[8] Siehe Richtlinie 2008/98/EG über Abfälle und zur Aufhebung bestimmter Richtlinien, die zuletzt durch die Richtlinie (EU) 2018/851 zur Änderung der Richtlinie 2008/98/EG über Abfälle geändert wurde

[9] Vgl. Deponieverordnung vom 27.4.2009, zuletzt am 30.6.2020 geändert

[10] Drucksache 20/8888, Deutscher Bundestag, 23.10.2023 (Bericht: Technikfolgenabschätzung – Chancen und Risiken der Digitalisierung kritischer kommunaler Infrastrukturen an den Beispielen der Wasser- und Abfallwirtschaft)

Speziell in der Abfallwirtschaft, gibt es verschiedene Maßnahmen und Pläne im Falle einer Krise. Die genauen Reaktionen hängen von der Art der Bedrohung, ihren Auswirkungen und dem spezifischen Krisenmanagementplan ab.

Im Bereich der Kritischen Infrastrukturen (KRITIS), speziell in der Abfallwirtschaft, gibt es verschiedene Maßnahmen und Pläne, die bei einem Angriff oder einer Pandemie ergriffen werden können. Die genauen Reaktionen hängen von der Art der Bedrohung, ihren Auswirkungen und dem spezifischen Krisenmanagementplan ab, der von den zuständigen Behörden und Organisationen entwickelt wurde. Hier sind einige mögliche Maßnahmen:

1. Kontinuitätsplanung:
Einrichtung von Kontinuitätsplänen, um sicherzustellen, dass grundlegende Abfallmanagement-Dienstleistungen aufrechterhalten werden können, selbst unter widrigen Bedingungen.

2. Ressourcenmobilisierung:
Identifikation und Bereitstellung zusätzlicher Ressourcen, um auf gesteigerte Bedarfe während einer Krise zu reagieren, z. B. Schutzausrüstung für Mitarbeiter, zusätzliche Fahrzeuge oder Anpassungen in der Müllentsorgungslogistik.

3. Kommunikation und Information:
Etablierung von klaren Kommunikationskanälen, um alle relevanten Stakeholder zu informieren, darunter Mitarbeiter, Vertragspartner, lokale Behörden und die Öffentlichkeit.

4. Hygiene- und Gesundheitsmaßnahmen:
Implementierung von erhöhten Hygiene- und Gesundheitsmaßnahmen für Mitarbeiter, um die Ausbreitung von Krankheiten zu minimieren.

5. Notfallpläne:
Erstellung von spezifischen Notfallplänen für verschiedene Szenarien, einschließlich Angriffe oder Pandemien, um eine koordinierte Reaktion zu gewährleisten.

6. Zusammenarbeit mit Behörden:
Zusammenarbeit mit lokalen und nationalen Behörden sowie anderen relevanten Organisationen*, um Informationen auszutauschen, Ressourcen zu koordinieren und ein gemeinsames Vorgehen zu planen.

„Andere relevante Organisationen“:

- Lokale, regionale und nationale Behörden, die für Umwelt- und Gesundheitsfragen zuständig sind.
- Gesundheitsbehörden, Krankenhäuser und medizinische Einrichtungen.
- Organisationen, die für den Katastrophenschutz und die Bewältigung von Notfällen verantwortlich sind.
- Andere Unternehmen oder Organisationen in der gleichen Branche oder geografischen Region, die möglicherweise Ressourcen teilen oder unterstützen können.
- NGOs, die in den Bereichen Umweltschutz, Gesundheit oder Katastrophenhilfe aktiv sind.
- Einrichtungen, die Forschung und Bildung im Bereich Umwelt- und Gesundheitsmanagement betreiben, können relevante Informationen und Expertise bereitstellen.
- Je nach der Art der Krise könnten die Weltgesundheitsorganisation (WHO) oder Umweltschutzagenturen mit in den Krisenstab eingebunden werden.

Eine frühzeitige Zusammenarbeit und Vorbereitung mit diesen Organisationen können dazu beitragen, die Resilienz und Effektivität der Krisenreaktion zu verbessern. Dies bedarf

natürlich einer Aufnahme in den Kriseninterventionsplan und kurzer Kommunikationswege bei einer Krise.

7. Logistik und Transport:
Anpassung von Logistik- und Transportplänen, um sicherzustellen, dass Abfall sicher und effizient entsorgt wird, auch unter erschwerten Bedingungen.

Sollten Logistik/Transport ausfallen, ist mit folgenden Herausforderungen zu rechnen:

1. Gesundheitsrisiken:
- Mangelnde Abfallentsorgung kann zu Ansammlungen von Müll führen, was die Verbreitung von Krankheiten durch Ungeziefer und Keime begünstigt.
- Ein Ausfall der Wasserversorgung kann zu sanitären Problemen führen, insbesondere wenn Menschen keinen Zugang zu sauberem Wasser für persönliche Hygiene und Trinkzwecke haben.

2. Umweltauswirkungen:
- Unkontrollierte Abfallansammlungen können Umweltauswirkungen haben (Boden- und Wasserverschmutzung)
- Ein Zusammenbruch der Wasserversorgung kann Ökosysteme beeinträchtigen und zu Wasserknappheit in der Umgebung führen.

3. Öffentliche Unruhen:
- Die Unzufriedenheit der Bevölkerung aufgrund von Abfallansammlungen oder Wasserknappheit kann zu Unruhen und sozialen Spannungen führen.

4. Gesundheitsversorgung:
- Ein Ausfall der Wasserversorgung beeinträchtigt Krankenhäuser und Gesundheitseinrichtungen, die auf Wasser angewiesen sind, um grundlegende Hygiene-standards aufrechtzuerhalten.

5. Wirtschaftliche Folgen:
- Unternehmen und die Wirtschaft insgesamt können unter den Auswirkungen von Abfallproblemen und Wasserknappheit leiden, da diese wesentliche Ressourcen für Produktionsprozesse darstellen.

6. Umweltkatastrophen:
- In einigen Fällen können Probleme in der Abfallwirtschaft zu Umweltkatastrophen wie Müllbränden oder illegaler Müllentsorgung führen. Letzteres kann dann zu Wasserverschmutzungen auch im Trinkwasserbereich führen.

7. Schwierigkeiten bei der Krisenbewältigung:
- Die Eindämmung von Krankheiten oder anderen Gesundheitskrisen kann durch unzureichende Abfallentsorgung und Wasserknappheit erschwert werden.

8. Soziale Folgen:
- Gemeinschaften können soziale Isolation und andere Belastungen erfahren, wenn grundlegende Dienstleistungen wie Wasser und Abfallmanagement nicht verfügbar sind. Hier sind weitere Spannungen intrafamiliär zu erwarten und es müssen evtl. Einsatzkräfte (Polizei, Rettungsdienst) für solche Streitigkeiten abgezogen werden, die an anderer Stelle für die Sicherung der Infrastruktur notwendig sind.

In Krisen ist es daher entscheidend, dass Krisenmanagementpläne für Abfallwirtschaft und Wasserversorgung existieren und dass schnell und effektiv von Seiten der Landesregierung reagiert wird.

Gibt es unterschiedliche Einstufungen für unterschiedliche Krisenszenarien?

Ob bestimmte Situationen und Entwicklungen als Krisen eingestuft werden, hängt von den Werten und Zielen der jeweiligen Beobachter ab und kann je nach Systemzugehörigkeit entsprechend gewichtet werden.

Eine Einstufung für unterschiedliche Krisenszenarien ist immer in der Gesamtheit der Krise zu betrachten. Welche weiteren Auswirkungen hat die aktuelle Krise. Welche weiteren Krisen können bei aktueller Krise/Krisenlage entstehen? Hier muss bei jeder Krise – unabhängig davon, welches Ausmaß sie hat – das Krisenmanagement durch eine saubere Krisenkommunikation mit Vorbereitung, Umsetzung und Nachsorge erfolgen. Alle Eventualitäten müssen eruiert werden, um bestens reagieren zu können. Das Ziel jedweden Krisenmanagements ist es initial zu reagieren, jedoch in der Folge (vorausschauend) zu *agieren*. Nur dadurch kann es gelingen, eine Krise zu bewältigen, ihre schwerwiegenden Folgen zu mindern oder zu beseitigen.

Im Katastrophenschutz gibt es, je nach Ereignis bzw. zu erwartendem Ereignis, entsprechende Alarmstufen.

Beispiel „Hochwassermeldepegel“:

Alarmstufe 1: (Meldebeginn) Beginnende Ausuferung von Gewässern
Ständige Beobachtung der meteorologischen Lage und der Hochwassersituation im Flussgebiet, einschließlich ihrer Entwicklungstendenzen, unter besonderer Berücksichtigung der Informationen des Landeshochwasserzentrums und des Wetterinformationssystems für den Katastrophenschutz (Deutscher Wetterdienst).

Alarmstufe 2: (Kontrolldienst) Beginnende Überflutung
Überflutung bzw. Überschwemmung land- oder forstwirtschaftlicher Flächen, Grünflächen, einschließlich Gärten und einzeln stehender Gebäude oder leichte Verkehrsbehinderung auf Straßen und Notwendigkeit der Sperrung von Wegen; Ausuferung bei eingedeichten Gewässern bis an den Deichfuß.

Zusätzlich zu Maßnahmen bei Alarmstufe 1: Alarmierung der zuständigen Einsatzkräfte und Herstellen ihrer Einsatzbereitschaft; laufende Kontrolle der Gewässer, Hochwasserschutzanlagen, gefährdeten Bauwerke und Ausuferungsgebiete; Weiterleitung von Informationen über festgestellte Gefährdungen und getroffene Abwehrmaßnahmen; Vorbereitung der aktiven Hochwasserbekämpfung; Vorbereitung von Evakuierungsmaßnahmen.

Alarmstufe 3: (Wachdienst) Überschwemmung bebauter Bereiche und der Infrastruktur
Überschwemmung von Teilen zusammenhängender Bebauung oder überörtlicher Straßen und Schienenwege; bei Volldeichen Wasserstand etwa in halber Deichhöhe, Vernässung von Polderflächen durch Drängewasser.

Zusätzlich zu Maßnahmen bei Alarmstufe 1 und 2: Vorbeugende Sicherungsmaßnahmen an Gefahrenstellen und Beseitigung örtlicher Gefährdungen und Schäden; Einrichtung von Einsatzstäben an Schwerpunkten der Hochwasserabwehr und Schaffung spezieller Nachrichtenverbindungen; Bereitstellung von Hochwasserschutzmaterialien an bekannten Gefahrenstellen; Bereitstellung einsatzbereiter Kräfte zur aktiven Hochwasserabwehr sowie

Anforderung und Vorbereitung weiterer Kräfte der Reserve; Beginn der Durchführung aktiver Hochwasserbekämpfungsmaßnahmen.

Alarmstufe 4: (Hochwasserabwehr) Gefahr für Leib und Leben
Überschwemmung größerer bebauter Gebiete mit sehr hohen Schäden, unmittelbare Gefährdung für Menschen und bedeutende Sachwerte; Wasserstand an Volldeichen im Freibordbereich mit unmittelbarer Gefahr der Überströmung oder unmittelbare Gefahr von Volldeichbrüchen.

Zusätzlich zu Maßnahmen bei Alarmstufe 1 bis 3:
Aktive Bekämpfung bestehender Gefahren für das Leben, die Gesundheit, die Versorgung mit lebensnotwendigen Gütern und Leistungen und für bedeutende Sachwerte.
Wie anhand des Alarmstufenbeispieles klar wird, sind immer vorausschauende zusätzliche Maßnahmen erforderlich. Vorausschau und Vorstellungen des Schlimmsten vom Schlimmen sorgen auch in der Krise für Prävention und somit für weitergehende Schadensabwehr.

Hat sich diese Einordnung in der Pandemie (SARS-CoV-2) bewährt?

Ja, während der Covid-19-Pandemie haben die Bundesländer unterschiedliche Einstufungen und Maßnahmen zur Krisenbewältigung implementiert, um die Verbreitung des Virus zu kontrollieren und die Auswirkungen auf die öffentliche Gesundheit, das Gesundheitswesen und die Gesellschaft zu minimieren. Einige der unterschiedlichen Einstufungen und Ansätze seien hier aufgelistet:

1. Regionalisierung und Lokalisierung:
Einige Länder haben regionale Ansätze zur Eindämmung des Virus verfolgt, wobei spezifische Maßnahmen auf Basis regionaler Infektionszahlen, Kapazitäten und Ressourcen (unter Berücksichtigung der Infrastruktur) umgesetzt wurden.

2. Farbcode-Systeme:
Einführen von Farbcode-Systemen, um den Schweregrad der Pandemie zu signalisieren. Verschiedene Farben repräsentieren unterschiedliche Restriktionen und Maßnahmen.

3. Stufenpläne:
Es gibt Stufenpläne, die verschiedene Maßnahmen je nach Infektionszahlen und anderen Faktoren vorsehen. Diese Pläne ermöglichen eine flexible Anpassung der Restriktionen.

4. Kombination von Maßnahmen:
Hier werden verschiedene Maßnahmen, wie Abstandsregelungen, Maskenpflicht (Reduzierung der Keimlast), Teststrategien, Impfungen und Kontaktverfolgung, um die Ausbreitung des Virus zu mildern, verfolgt.

5. Impfstrategien:
Es wurden unterschiedliche Impfstrategien verfolgt, indem sie Prioritäten für bestimmte Bevölkerungsgruppen festlegten. Somit wurden gezielt unterschiedliche Impfgeschwindigkeiten erreicht.

6. Frühzeitiges Handeln:
Länder, die frühzeitig und proaktiv auf steigende Infektionszahlen reagierten, haben erfolgreichere Ergebnisse bei der Eindämmung der Pandemie erzielt (z.B.: Neuseeland, Taiwan und Südkorea)[11] als Länder die in ihrem Handeln zögerten (z.B.: China oder Schweden).

[11] Siehe Studie: "Early epidemiological indicators, outcomes, and interventions of COVID-19 pandemic: A systematic review"; U. Patel, P. Malik, D. Mehta, D. Shah, R. Kelkar, C. Pinto, M. Suprun, M. Dhamoon, N. Hennig, H. Sacks; https://pubmed.ncbi.nlm.nih.gov/33110589/

7. Kommunikation:
Länder mit klaren, konsistenten und transparenten Kommunikationsstrategien haben eine größere Akzeptanz der Bevölkerung für die implementierten Maßnahmen erreicht.

Der Erfolg von Maßnahmen hängt grundsätzlich von der Umsetzung, der Zusammenarbeit und der Anpassungsfähigkeit der Bevölkerung ab. Die Länder haben im Laufe der Pandemie ihre Strategien immer wieder angepasst, um quasi „Just in Time" erfolgreich zu agieren.

Anmerkung zur SARS-CoV-2-Pandemie:
Es ist mit hoher Wahrscheinlichkeit damit zu rechnen, dass die Corona-Pandemie nicht die letzte ihrer Art gewesen sein wird. Daher erscheint es dringend geboten, eine gründliche und umfassende Aufarbeitung der Erfahrungen und Maßnahmen vorzunehmen, um zukünftig unser Gesundheitswesen besser auf Pandemien und Epidemien vorzubereiten. Eine solche Aufarbeitung darf nicht vor dem deutschen Gesundheitswesen Halt machen! Je besser das Gesundheitssystem in seinem Normalzustand funktioniert, umso resilienter und handlungsfähiger ist es in Krisen- und Ausnahmezeiten aufgestellt.
Betrachten wir jedoch den Status Quo im Gesundheitswesen, so sind bereits heute strukturelle und funktionale Mängel vorhanden, die dem Normalzustand Probleme bereiten. Sei es die unzureichende personelle und sachliche Ausstattung der öffentlichen Gesundheitsdienste (Gesundheitsämter) oder die vielen Kliniken mit ihrer unzureichenden Personalbesetzung im intensivmedizinischen Bereich und der Folge von Bettenschließungen. Hinzu kommen immer wieder Engpässe von wichtigen Medikamenten oder Lieferschwierigkeiten von dringend notwendigen Verbrauchsmaterialien für die Patientenversorgung oder -diagnostik. Somit ist das gesamte Gesundheitssystem auf den Prüfstand zu stellen und dies nicht nur im Blick auf die durchgemachte oder eine eventuell zukünftige Pandemie. Stellen Sie sich daher bitte die Frage, ob das gegenwärtige Gesundheitssystem einen Normalzustand aufweist, welcher in seiner Art und Weise den berechtigten Erwartungen der Bevölkerung entspricht. Wenn ein System bereits im Normalzustand kränkelt, wie soll es dann seinen „gesunden" Schutz in einer Krise entfalten können?

Welche Auswirkungen sind durch Funktionseinschränkungen im Bereich KRITIS zu erwarten?

Funktionseinschränkungen in den Kritischen Infrastrukturen (KRITIS) können erhebliche Auswirkungen auf verschiedene Bereiche der Gesellschaft haben. Hier sind einige potenzielle Auswirkungen:

1. Öffentliche Gesundheit:
Funktionseinschränkungen im Gesundheitswesen können den Zugang zu medizinischer Versorgung, Arzneimitteln und anderen Gesundheitsdienstleistungen beeinträchtigen.

2. Sicherheit:
Einschränkungen im Bereich der öffentlichen Sicherheit, einschließlich Polizei und Rettungsdienste, können die Fähigkeit zur Bewältigung von Notfällen und die Aufrechterhaltung der öffentlichen Ordnung beeinträchtigen. Diebstahl/Plünderung sind zu erwarten.

3. Energieversorgung:
Einschränkungen in der Energieversorgung können zu Stromausfällen führen, was wiederum Auswirkungen auf Wohnungen, Unternehmen und kritische Einrichtungen hat.

4. Wasserversorgung:
Funktionseinschränkungen in der Wasserversorgung können zu Wasserknappheit, hygienischen Problemen und Beeinträchtigungen der sanitären Anlagen führen.

5. Transport und Verkehr:
Beeinträchtigungen im Transportwesen können den Verkehr behindern, was Auswirkungen auf den Güter- und Personenverkehr sowie auf die Lieferketten hat. Zapfsäulen funktionieren nicht, sodass das Transportwesen brachliegt, weil kein Treibstoff großflächig getankt werden kann. Und wenn durch Ersatztankmaßnahmen Transport und Logistik aufrechterhalten werden können, dann in massiv zeitlich verzögertem Rahmen, da die Fahrzeuge Umwege fahren müssen, um überhaupt an Treibstoff zu gelangen. Hier wäre auch die Frage nach der Ressource: Tankfahrzeuge.

6. Telekommunikation:
Einschränkungen in der Telekommunikation können die Kommunikation beeinträchtigen und die Fähigkeit der Menschen zur Informationsbeschaffung und -verbreitung verringern. Durch mangelnde Informationsbeschaffung könnten Gegenpole in der Bevölkerung entstehen, welche „Negativpropaganda" betreiben und somit die Betroffenen verunsichern.

7. Finanzsystem:
Funktionseinschränkungen im Finanzsektor können zu Störungen bei Zahlungsabwicklungen, Bankdienstleistungen und anderen Finanztransaktionen führen. Menschen können weder mit der Karte noch mit Bargeld zahlen. Strom-/IT-Ausfall ➔ nur Bargeld möglich. Kein Bargeld vorhanden oder kurzfristig aufgebraucht, da Geldautomaten nicht funktionieren.

8. Lebensmittelversorgung:
Beeinträchtigungen in der Lebensmittelproduktion und -verteilung können zu Versorgungsproblemen und Engpässen führen.

9. Digitale Infrastruktur:
Funktionseinschränkungen in der digitalen Infrastruktur können zu Störungen in der Informationstechnologie, Cybersicherheitsproblemen und Datenverlust führen.

10. Wirtschaft:
Beeinträchtigungen in kritischen Wirtschaftssektoren können zu Produktionsausfällen, Arbeitsplatzverlusten und wirtschaftlicher Instabilität führen.

11. Gesellschaftliches Vertrauen:
Funktionseinschränkungen können das Vertrauen der Bevölkerung in die Fähigkeit der Regierung und der Kritischen Infrastrukturen zur Bewältigung von Krisen beeinträchtigen.

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

Pandemien:

1. Gesundheitswesen: Überlastung von Krankenhäusern, Personalmangel. Medikamentenmangel, Versorgungsmangel, Materialmangel. Hohe Mortalitätsrate durch Defizite der vorbezeichneten Engpässe. Hohe Belastung der psychischen Gesundheit.[12] [13]

2. Energieversorgung: Reduzierte Arbeitskraft, Verzögerungen bei Wartungsarbeiten, Hitzetod, Erfrierungstod.

[12] Siehe: https://www.bundestag.de/resource/blob/895608/d76c06ceba31d5a3401ffc1f3268de79/WD-9-018-22-pdf-data.pdf

[13] Siehe: https://library.oapen.org/handle/20.500.12657/54041; Krankenhaus-Report 2022; J. Klauber, J. Wasem, A. Beivers, C. Mostert, Springer-Verlag;

3. Wasserversorgung: Einschränkungen bei Wartung und Betrieb, Verdurstung, Tod.

4. Transport und Verkehr: Beeinträchtigungen durch Lockdowns und Quarantänen, Nahrungsmangel, Hunger, Hungertod.

5. Telekommunikation: Erhöhte Nachfrage, mögliche Engpässe. Keine Kommunikation, Mangel an Kommunikation.

6. Lebensmittelversorgung: Produktionsausfälle und Logistikprobleme. Warenmangel, Plünderung, Hunger, Hungertod. Verdurstung; Unterernährung.

Extremwetterereignisse:

1. Energieversorgung: Stromausfälle durch Sturm- oder Überschwemmungsschäden.

2. Wasserversorgung: Wasserknappheit durch Dürre oder Überschwemmungen.

3. Transport und Verkehr: Straßensperrungen, Unterbrechungen im Flug- und Schienenverkehr.

4. Telekommunikation: Beschädigung von Infrastruktur, Ausfall von Netzwerken.

5. Lebensmittelversorgung: Ernteausfälle, Logistikprobleme.

6. Digitale Infrastruktur: Cybersicherheitsrisiken durch Extremwetterereignisse.

Folgend, wie unter Pandemie beschrieben: Versorgungsdefizite, anhaltende Versorgungsdefizite sorgen für Eskalation, Gewalt, Tötung bzw. Versterben von Menschen.

****

KRITIS

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

Die Kritischen Infrastrukturen werden im Fall einer Krise durch bestimmte Ereignisse oder Umstände in einen Krisenmodus versetzt.

1. Auslöser für den Krisenmodus:

1.1. Erhebliche Störungen oder Schäden:

- Schwere Naturkatastrophen (z. B. Erdbeben, Überschwemmungen, Stürme).
- Technische Unfälle (z. B. Chemieunfälle, Nuklearkatastrophen).
- Große Cyberangriffe oder Sicherheitsverletzungen.

1.2. Pandemien und Gesundheitskrisen:

- Schnelle Verbreitung von ansteckenden Krankheiten.
- Hohe Auslastung des Gesundheitssystems.

1.3. Sicherheitsbedrohungen:

- Terroranschläge oder Bedrohungen der nationalen Sicherheit.
- Große Sicherheitsverletzungen.

1.4. Versorgungsausfälle:

- Energieausfälle oder Versorgungsengpässe.
- Unterbrechungen in der Wasserversorgung oder Lebensmittelversorgung.

2. Auswirkungen des Krisenmodus:

2.1. Aktivierung von Krisenmanagementplänen:

- Umsetzung vordefinierter Maßnahmenpläne zur Bewältigung der Krise.

2.2. Intensivierung von Überwachung und Kommunikation:

- Erhöhte Überwachung von Systemen und Ressourcen.
- Intensive Kommunikation zwischen relevanten Behörden und Organisationen.

2.3. Ressourcenmobilisierung:

- Schnelle Bereitstellung zusätzlicher Ressourcen, einschließlich Personal und Ausrüstung.

2.4. Anpassung von Betriebsabläufen:

- Anpassung von Betriebsabläufen, um die kritischen Dienstleistungen aufrechtzuerhalten.

2.5. Zusammenarbeit mit Behörden:

- Engere Zusammenarbeit mit lokalen, regionalen und nationalen Behörden.

2.6. Einschränkungen und Schutzmaßnahmen:

- Umsetzung von Schutzmaßnahmen für Mitarbeiter und die Bevölkerung.
- Einschränkungen, um die Verbreitung von Gefahren zu minimieren.

2.7. Öffentliche Kommunikation:

- Klare und regelmäßige Kommunikation mit der Öffentlichkeit, um Informationen bereitzustellen und Anweisungen zu geben.

Die genauen Auswirkungen und Maßnahmen können je nach Art der Krise und der spezifischen Kritischen Infrastrukturen variieren. Der Krisenmodus ist darauf ausgerichtet, eine koordinierte und effektive Problemlösung zu gewährleisten und die Auswirkungen auf das Funktionieren der Gesellschaft einzugrenzen

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?

Die Festlegung von konkreten Schwellenwerten variiert je nach Region und spezifischem Kontext. In vielen Fällen sind solche Schwellenwerte in offiziellen Richtlinien und Krisenmanagementplänen definiert. Die Kriterien können sich auf verschiedene Faktoren beziehen, einschließlich der Schwere eines Ereignisses, der Bedrohung für die Bevölkerung, der Auswirkungen auf Kritische Infrastrukturen und anderer relevanter Aspekte.

Eine gesetzliche Festlegung ist abzulehnen. Durch eine zu starre Gesetzgebung wird die regionalspezifische Entscheidung eingeschränkt.

Beispiele für Kriterien, die bei der Festlegung von Schwellenwerten berücksichtigt werden können:

1. Gesundheitskrisen:
- Anzahl der Infizierten, Hospitalisierungen und Todesfälle.
- Kapazitätsüberschreitungen im Gesundheitswesen.

2. Naturkatastrophen:
- Ausmaß von Überschwemmungen, Erdbeben oder Stürmen.
- Schäden an Kritischen Infrastrukturen.

3. Technische Unfälle:
- Schweregrad und Ausmaß von Chemieunfällen oder nuklearen Vorfällen.
- Gefährdung von Bevölkerung und Umwelt.

4. Sicherheitsbedrohungen:
- Art und Ausmaß von terroristischen Aktivitäten.
- Bedrohung der nationalen Sicherheit.

Die Definition von Schwellenwerten ist komplex und erfordert eine ganzheitliche Bewertung von verschiedenen Faktoren. Flexibilität ist in den Kriterien zu berücksichtigen, um sich an die ändernden Umstände anzupassen.

Die Festlegung von Schwellenwerten muss im Einklang mit Sicherheitsstrategien und Krisenmanagementplänen stehen. Solche Schwellenwerte gehören regelmäßig überprüft und müssen bei Bedarf aktualisiert werden (Sicherstellung der Relevanz).
Schwellenwerte müssen von den regionalen Behörden, in Zusammenarbeit mit den überregionalen Behörden individuell erstellt werden. Konkret bedeutet dies, dass die Städte und Landkreise ihre Schwellenwerte durch Experten (Kompetenzteam Katastrophenschutz) definieren lassen und die jeweils zuständige Bezirksregierung hier involviert ist. Somit kann die jeweilige Bezirksregierung in ihrem Bereich im Falle einer Krise regional übergreifend agieren, unterstützen und koordinieren. Die Bezirksregierungen arbeiten grundsätzlich alle mit dem Innenministerium NRW (Kompetenzteam Katastrophenschutz) eng zusammen, um Landeskrisen zu bewältigen.

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?

Das in 2021 von Innenminister Herbert Reul berufene Kompetenzteam Katastrophenschutz mit seinen erfahrenen Experten aus verschiedenen Organisationen und Verbänden reicht als Beratungsteam völlig aus, um Szenarien für zukünftige Krisenereignisse zu evaluieren und entsprechende Sicherheitspläne der Kritischen Infrastruktur zu erarbeiten.

Mit dem Beratungsgremium werden die wichtigsten Probleme im Katastrophenschutz benannt und Empfehlungen zur Weiterentwicklung erarbeitet bzw. aktualisiert und an die präsenten Herausforderungen angepasst.

Maßnahmen und Rollenverteilungen der Aufgaben im Falle eines Krisenereignisses werden ausreichend durch das BMI und den Katastrophenschutz NRW (Innenministerium NRW) abgedeckt.

Entsprechende Abfolgepläne, Bedarfspläne, Umsetzungspläne sind vorhanden. Diese gehören lediglich stringent umgesetzt. Hier ist nicht die Organisation und die Dienstabfolge das Problem, sondern die Rekrutierung von ausreichendem Personal zur Bewältigung der Krise.

Oder auf „gut Deutsch“: Man kann sich „totregulieren“ und Vorgaben ohne Ende schreiben – es nützt nichts, wenn es an Personal mangelt.

Von daher ist bei einer Krise in NRW – sofern die anderen Länder nicht betroffen sind – der Bund frühzeitig um Unterstützung zu bitten. Denn Zeitgewinn bedeutet weniger Verlust von Leben und Gütern sowie weniger finanzielle Schäden.

Wie ist im Bereich KRITIS die Kommunikationsstruktur auf EU-, Bund-, Länder- und kommunaler Ebene organisiert? Gibt es dort aus Ihrer Sicht Verbesserungsbedarf und wenn ja, was empfehlen Sie?

Zur Europäischen Union:

Forderung der Europäischen Union:
EU-Mitgliedsstaaten müssen kritische Einrichtungen besser vor Naturgefahren, Sabotage und Cyberangriffen schützen.

Hierzu gibt es die EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie). Die **CER-Richtlinie**[14] verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotage zu stärken.

Außerdem gibt es die **NIS-2-Richtlinie**[15] für ein hohes gemeinsames Cybersicherheitsniveau in der EU. Die NIS-2-Richtlinie weitet Cybersicherheitsvorgaben auf mehr Sektoren und mehr Unternehmen aus. Betroffene Unternehmen werden nur noch anhand ihrer

[14] https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[15] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Unternehmensgröße erfasst. Das gilt grundsätzlich für alle mittleren- und Großunternehmen in den betroffenen Wirtschaftssektoren.

Mit den Richtlinien will die EU einen einheitlichen Schutz vor physischen Störungen und Cyberangriffen gewährleisten. So sind die erfassten Sektoren weitgehend identisch: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung und Weltraum (*European Union Space Programme)*.[16]

Von der NIS-2-Richtlinie erfasste Unternehmen müssen zukünftig Risikomanagementmaßnahmen im Cybersicherheitsbereich vorweisen und Meldepflichten im Fall von Cybervorfällen erfüllen. Nach Schätzungen des Statistischen Bundesamts betrifft das in Deutschland insgesamt rund 29.000 Unternehmen – mehr als fünfmal so viele wie zuvor.

Die CER-Richtlinie wird durch das im Koalitionsvertrag vereinbarte **KRITIS-Dachgesetz**[17] umgesetzt. Das Gesetz schafft erstmalig eine sektorenübergreifende bundesgesetzliche Regelung zum physischen Schutz Kritischer Infrastrukturen in Deutschland (Stand 01/2023).

Was macht das KRITIS-Dachgesetz?

- Kritische Infrastrukturen sollen klar und systematisch identifiziert werden.
- Staat und KRITIS-Betreiber sollen regelmäßige Risikobewertungen durchführen und dadurch Gefahren besser erkennen.
- Es werden Mindeststandards für Betreiber Kritischer Infrastrukturen festgelegt. Für die Betreiber bedeutet das mehr Handlungssicherheit, um sich gegen Gefahren zu schützen.
- Ein zentrales Meldesystem für Störungen soll das bestehende Meldewesen im Cybersicherheitsbereich ergänzen. Mögliche Schwachstellen beim Schutz Kritischer Infrastrukturen können so besser erkannt und behoben werden.
- Die Zusammenarbeit der beteiligten Akteure im Bereich der Kritischen Infrastrukturen soll besser organisiert und klare Verantwortlichkeiten und Ansprechpartner benannt werden.

Innerhalb der Europäischen Union wird über die jeweiligen Bundesministerien bzw. Innenministerien kommuniziert, die für den Katastrophenschutz verantwortlich sind. Im Regelfall sollten Amtshilfeersuchen über das Auswärtige Amt erfolgen.

Die genaue Kommunikationsstruktur kann je nach EU-Mitgliedstaat und Sektor variieren und ist auf verschiedenen Ebenen verteilt. Wichtig bei alledem ist eine effektive Kommunikation auf diesen Ebenen, um im Falle von Bedrohungen oder Vorfällen eine koordinierte Reaktion zu gewährleisten.

Als Beispiel sei hier die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) erwähnt. ENISA ist die EU-Agentur für Netz- und Informationssicherheit. Sie unterstützt die EU-Mitgliedstaaten bei der Verbesserung ihrer Fähigkeiten im Bereich Cybersicherheit, einschließlich des Schutzes Kritischer Infrastrukturen. ENISA spielt eine Rolle bei der Koordinierung und dem Austausch bewährter Praktiken im Bereich Cybersicherheit und ist innerhalb der EU zentraler Ansprechpartner bei Krisen im Bereich der Netz- und Informationssicherheit.

[16] Navigationssystem Galileo, Copernicus-Programm der globalen Beobachtungssatelliten und EGNOS; European Geostationary Navigation Overlay Service (EGNOS) ist ein europäisches Differential Global Positioning System (DGPS) als Erweiterungssystem zur Satellitennavigation: https://www.eca.europa.eu/lists/ecadocuments/sr21_07/sr_eus-space-assets_de.pdf

[17] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/01/eu-richtlinien-kritis.html

Kommunikationsstruktur innerhalb des Bundes:

Innerhalb der Bundesregierung koordiniert das Bundesinnenministerium die Aktivitäten, Strategien und Maßnahmen zum bestmöglichen Schutz der Kritischen Infrastruktur. Dafür hat im Oktober 2022 ein **Gemeinsamer Koordinierungsstab Kritische Infrastruktur (GEKKIS)**[18] seine Arbeit aufgenommen.

Dieser soll:

- die aktuellsten Lagebilder zum Schutz Kritischer Infrastrukturen zur Verfügung stellen. So haben alle Ministerien einen ressortübergreifenden Überblick über die aktuelle Gefährdungslage.
- einen strukturierten Austausch der Ressorts ermöglichen, um gemeinsame Herausforderungen zu identifizieren und zusammen an deren Bewältigung zu arbeiten.
- als Ad-hoc-Gruppe bei relevanten Vorfällen unmittelbar zusammenkommen. Mit der bestehenden Notfall-Infrastruktur des BMI-Lagezentrums wird eine 24/7-Erreichbarkeit von Entscheidungsträgern und Entscheidungsträgerinnen in den relevanten Ministerien sichergestellt.

Wie im Koalitionsvertrag der Bundesregierung vereinbart, erhöht das **KRITIS-Dachgesetz**[19] die Anforderungen an die Betreiber Kritischer Infrastrukturen. Grundsätzlich sind in Deutschland die Betreiber verantwortlich für den Schutz ihrer Anlagen. Diese müssen sich umfassend gegen Gefahren wie Naturkatastrophen, Terrorismus, Sabotage, aber auch menschliches Versagen wappnen. Gleichzeitig werden Meldepflichten für Sicherheitsvorfälle und Berichtspflichten für Infrastrukturbetreiber etabliert.

Fachlich wird das BMI bei dem Schutz Kritischer Infrastruktur unterstützt:

- vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK);
- vom Bundesamt für Sicherheit in der Informationstechnik (BSI);
- und von der Bundesanstalt Technisches Hilfswerk (THW).

Fazit:
Der deutsche Rechtsrahmen für den Schutz Kritischer Infrastrukturen wird somit in ein europäisches Gesamtsystem eingebettet. Durch europaweit einheitliche Mindestvorgaben und verstärkte grenzüberschreitende Kooperation wird die Versorgungssicherheit in Deutschland und in Europa gestärkt. Die Stärkung der Resilienz Kritischer Infrastrukturen wird darüber hinaus auch auf Ebene der NATO als Ziel verfolgt.

Kommunikationsstruktur auf Länderebene und kommunaler Ebene:

Auf **Landesebene** sowie auf kommunaler Ebene erfolgt die Kommunikation im Bereich Kritischer Infrastrukturen (KRITIS) über verschiedene Institutionen und Mechanismen.

Nordrhein-Westfalen (NRW):

1. Ministerium des Innern des Landes Nordrhein-Westfalen
(bereits anderweitig erläutert)

[18] https://www.bmi.bund.de/DE/service/lexikon/functions/bmi-lexikon.html?cms_lv2=9391112&cms_lv3=9398156#doc9398156
[19] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/nachrichten/2022/eckpunkte-kritis.pdf?__blob=publicationFile&v=1

2. Landesamt für Zentrale Polizeiliche Dienste (LZPD): Das LZPD ist zuständig für die Zusammenarbeit mit den Kommunen und für koordinierte Maßnahmen zur Gewährleistung der öffentlichen Sicherheit.

3. Landesamt für Information und Technik Nordrhein-Westfalen (IT.NRW): IT.NRW kann eine Rolle bei der technischen Unterstützung und Datenaustausch in Bezug auf Kritische Infrastrukturen spielen.

4. Kommunen und Landkreise: Die Kommunen und Landkreise in NRW haben eigene Zuständigkeiten und Verantwortlichkeiten im Bereich KRITIS. Einsatz der kommunalen Krisenstäbe bei der regionalen Koordination und Kommunikation.

Auf kommunaler Ebene:

1. Kommunale Krisenstäbe:
Die Kommunen (Städte und Landkreise) in NRW verfügen über eigene Krisenstäbe, die im Falle von Krisen oder besonderen Ereignissen aktiviert werden können. Diese Stäbe koordinieren die Maßnahmen vor Ort.

2. Integrierte Leitstellen:
Integrierte Leitstellen sind zuständig für die Koordination von Rettungsdiensten, Feuerwehr und Polizei. Sie spielen eine wichtige Rolle in der Kommunikation und Koordination während Notfällen.

3. Landeszentrale für Sicherheit in der Informationstechnik (LZSI):
Die LZSI in NRW kann eine Rolle in der Sensibilisierung, Schulung und Koordination im Bereich der Informationssicherheit, einschließlich KRITIS, spielen.

Die Kommunikation erfolgt durch regelmäßige Treffen, Schulungen, Übungen und den Austausch von Informationen zwischen den beteiligten Institutionen. Die genaue Kommunikationsstruktur kann je nach Größe und Organisation der Kommune variieren, jedoch ist eine enge Zusammenarbeit und Koordination zwischen allen entscheidend, um eine effektive Krisenbewältigung sicherzustellen.

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

Die Einschätzung zum Verbesserungsbedarf im Bereich Kritischer Infrastrukturen (KRITIS) ist ständigen Veränderungen und Entwicklungen unterworfen. Von daher ist es wichtig, durch entsprechende Arbeits- und Kompetenzgruppen auf dem aktuellsten Stand zu sein. Es darf bei der Bewältigung von Krisen nicht nur ein umfassendes und schnelles Handeln mit vorhandenen Ablaufplänen vorliegen. Es müssen in regelmäßigen Abständen auch die Gesamtbedingungen (Krise, Schutz, Vorsorge, Status Quo) überprüft und ggf. angepasst werden.
Hierzu gehören beispielsweise die Einführung neuer Technologien und Innovationen, um den Schutz Kritischer Infrastrukturen kontinuierlich zu verbessern sowie regelmäßige Schulungen und Übungen für Personal in Kritischen Infrastrukturen, um die Reaktionsfähigkeit in Krisensituationen zu verbessern. Auch gehört die Stärkung der Kommunikation und des Informationsaustauschs zwischen verschiedenen Ebenen (lokal, regional, national) zu dem kontinuierlichen Verbesserungsprozess (KVP). Im Sinne des KVP bedarf es natürlich auch der Anpassung des rechtlichen Rahmens und somit auch im Bedarfsfall individueller Gesetzesänderungen. Daraus folgt die Anpassung und Aktualisierung der rechtlichen Rahmenbedingungen, um auf neue Herausforderungen und Entwicklungen angemessen reagieren zu können.

Ein weiterer Aspekt wäre die Erhöhung der Sensibilisierung der Bevölkerung für die Bedeutung von Kritischen Infrastrukturen und Förderung der Beteiligung von Bürgern an Sicherheitsmaßnahmen (siehe auch Beantwortung der Frage „Welche Rolle spielt die Bevölkerung für die Resilienz Kritischer Infrastruktur?“).

Wie ist die Vulnerabilität der kritischen Infrastrukturen einzuschätzen?

Einschätzung der Vulnerabilität Kritischer Infrastrukturen:

Physische Sicherheit:
Standorte, Gebäude und Infrastruktur können anfällig für physische Angriffe oder Naturkatastrophen sein. Dies schließt auch den Schutz vor unbefugtem Zugang oder Sabotage ein.

Cybersicherheit:
Schwächen in den IT-Systemen, unzureichende Sicherheitsmaßnahmen und Mängel in der Netzwerkinfrastruktur können die Cyber-Resilienz beeinträchtigen.

Personelle Sicherheit:
Mangelnde Schulung und Sensibilisierung des Personals für Sicherheitsrisiken kann zu menschlichem Versagen führen und die Gesamtsicherheit beeinträchtigen. Im Rahmen der Sabotage kann Personal erpresst bzw. bedroht werden, um Schadensmaßnahmen durchzuführen. Terroristen können sich einstellen lassen und tarnen, umso Angriffe von innen vorzubereiten.

Lieferketten:
Abhängigkeit von komplexen Lieferketten kann zu Unterbrechungen führen, wenn eine Komponente oder ein Dienstleister Schwierigkeiten hat bzw. ausfällt.

Kommunikationssysteme:
Störungen oder Ausfälle von Kommunikationssystemen können die Reaktionsfähigkeit in Krisensituationen beeinträchtigen.

Abhängigkeit von Technologie:
Die zunehmende Integration von Informationstechnologie in Kritische Infrastrukturen erhöht die Anfälligkeit für technische Störungen, Cyberangriffe und komplexe technologische Risiken.

Regulatorische Compliance:
Nichteinhaltung von Sicherheitsstandards und gesetzlichen Vorschriften kann die Vulnerabilität erhöhen.

Natürliche Risiken:
Geografische Lage und Exposition gegenüber Naturgefahren wie Hochwasser, Erdbeben oder Stürmen können die Vulnerabilität beeinflussen.

Gemeinsame Abhängigkeiten:
Gemeinsame Infrastrukturen und Dienstleister können zu gemeinsamen Schwachstellen führen, da mehrere Sektoren miteinander verbunden sind.

Bei alledem sind auch Phasen der Arbeitsniederlegung (Streik) kritisch zu betrachten. Die Kritische Infrastruktur wird dadurch vulnerabel. Sollten in diesen Zeitraum Angriffe von innen oder außen durchgeführt werden, so ist das Sicherungssystem evtl. nicht vollständig aktiv.

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

Aufgrund ihrer zentralen Rolle in der Aufrechterhaltung essenzieller Dienstleistungen gehören die Mitarbeiter Kritischer Infrastrukturen unter besonderen Schutz gestellt. Dieser Schutz erstreckt sich auf verschiedene Aspekte, darunter physische Sicherheit, Cybersicherheit, Gesundheitsschutz und Sicherheit am Arbeitsplatz.

Physische Sicherheit:
Mitarbeiter in Kritischen Infrastrukturen, insbesondere solche, die physische Standorte betreuen, müssen vor potenziellen Bedrohungen, einschließlich unbefugten Zugangs oder Angriffen, geschützt werden. Dies erfordert angemessene Sicherheitsmaßnahmen und Zugangskontrollen.

Cybersicherheit:
Angemessene Schulung und Sensibilisierung der Mitarbeiter für Cybersicherheitsrisiken sind wichtig, um die Auswirkungen von Cyberangriffen zu minimieren. Dies kann den Schutz vor Phishing, Social Engineering und anderen Cyberbedrohungen umfassen.

Gesundheitsschutz und Sicherheit am Arbeitsplatz:
Kritische Infrastrukturen müssen sicherstellen, dass die Arbeitsplätze ihrer Mitarbeiter sicher und gesund sind. Dies schließt die Einhaltung von Gesundheits- und Sicherheitsstandards ein, um Unfälle und gesundheitliche Risiken zu minimieren.

Krisenbewältigung und Notfallvorsorge:
Mitarbeiter sollten in Notfallverfahren und Krisenbewältigungsplänen geschult sein, um angemessen auf unvorhergesehene Ereignisse, etwa Naturkatastrophen oder Cyberangriffe, reagieren zu können.

Schutz vor Diskriminierung und Übergriffen:
Der Schutz der Mitarbeiter umfasst auch den Schutz vor Diskriminierung, Mobbing oder Übergriffen am Arbeitsplatz.

Schutz vor gesundheitlichen Risiken:
Insbesondere in Krisenzeiten wie Pandemien ist der Schutz vor gesundheitlichen Risiken, etwa mittels Schutzausrüstung und Gesundheitsvorsorge, von besonderer Bedeutung.

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

Die Covid-19-Pandemie hat verschiedene Erkenntnisse im Zusammenhang mit der Sicherheit und dem Schutz der Mitarbeiter, insbesondere in Kritischen Infrastrukturen, hervorgebracht.

Hierzu möchte ich einige Beispiele auflisten (Erkenntnis + Umsetzung):

Flexibles Arbeitsmodell:
Erkenntnis: Die Pandemie hat die Notwendigkeit eines flexibleren Arbeitsmodells unterstrichen, einschließlich Telearbeit und Homeoffice, um die Kontinuität der Arbeit zu gewährleisten.

Umsetzung: Organisationen haben verstärkt auf flexible Arbeitsarrangements gesetzt, um den Mitarbeitern die Möglichkeit zu geben, von zu Hause aus zu arbeiten.

Digitale Transformation:
Erkenntnis: Die Pandemie hat die Bedeutung der Digitalisierung und Informationstechnologie für die Geschäftskontinuität hervorgehoben.

Umsetzung: Beschleunigung digitaler Transformationsprojekte, einschließlich Cloud-basierter Lösungen, um die Widerstandsfähigkeit gegenüber Störungen zu erhöhen.

Gesundheits- und Sicherheitsmaßnahmen:
Erkenntnis: Schutzmaßnahmen am Arbeitsplatz sind entscheidend, um die Gesundheit der Mitarbeiter zu gewährleisten.

Umsetzung: Implementierung von Hygienemaßnahmen, Bereitstellung von Schutzausrüstung, Einhaltung von Abstandsregeln und verstärkte Reinigungspraktiken am Arbeitsplatz.

Kommunikation und Krisenmanagement:
Erkenntnis: Eine klare Kommunikation ist in Krisensituationen von entscheidender Bedeutung.

Umsetzung: Verbesserte Kommunikationsstrategien, regelmäßige Updates für Mitarbeiter und klare Anweisungen für den Umgang mit Krisensituationen.

Mitarbeiterunterstützung und Wohlbefinden:
Erkenntnis: Die psychische Gesundheit der Mitarbeiter ist ein wichtiger Faktor für die Resilienz in Krisenzeiten.

Umsetzung: Einführung von Programmen zur Unterstützung der psychischen Gesundheit, Schaffung von Ressourcen für die Bewältigung von Stress und emotionalen Belastungen.

Risikobewertung und Business Continuity:
Erkenntnis: Eine gründliche Risikobewertung und ein effektives Business Continuity Management sind von entscheidender Bedeutung.

Umsetzung: Überprüfung und Aktualisierung von Risikobewertungen, verstärkte Betonung der Geschäftskontinuitätsplanung.

Grenzübergreifende Zusammenarbeit:
Erkenntnis: Grenzübergreifende Zusammenarbeit und Austausch bewährter Praktiken sind entscheidend.

Umsetzung: Intensivierung der Zusammenarbeit zwischen Organisationen, Behörden und Branchen auf nationaler und internationaler Ebene.

Retrospektiv haben die Mitarbeiter der gesamten Kritischen Infrastruktur während der Pandemie Höchstleistungen sowie eine erhöhte Arbeitsbereitschaft mit Mehrarbeit gezeigt.

Bedauerlicherweise ist grundsätzlich während jeder Krise in den Bereichen der Kritischen Infrastruktur ein Rückgang von Berufstätigen zu verzeichnen. Hier kommt es wegen Reduk-

tion der beruflichen Resilienz in der Akutsituation zur Flucht aus dem Beruf, um vor der Krise zu „fliehen“. Dies ist ein natürliches psychologisches Phänomen, welches bei jedem kritischen Ereignis zu berücksichtigen ist.
So gab es im Gesundheitsbereich während der Covid-19-Pandemie Einbrüche in der Patientenversorgung, da Pflegekräfte in der Pandemiezeit mit der exorbitanten Belastung während des Dienstes überfordert waren. Die Folge war ein erhöhter Krankenstand (nicht wegen eigener Covid-Infektion) sowie auch vermehrte Kündigungen in den Pflegeberufen (siehe hierzu Abbildung 3 auf der folgenden Seite).

Somit ist auch klar, dass die Resilienz der Bevölkerung **im Berufsleben** eine große Rolle für die Sicherheit von Kritischen Infrastrukturen darstellt.

Aber auch im Privatbereich haben die Menschen mit großer Resilienz im Falle einer Krise bessere Überlebenschancen. Sie agieren rationaler, weniger emotional, und besitzen eine größere Compliance als Menschen mit geringer Resilienz. (siehe auch: „Welche Rolle spielt die Resilienz der Bevölkerung für die Sicherheit von Kritischen Infrastrukturen?“)

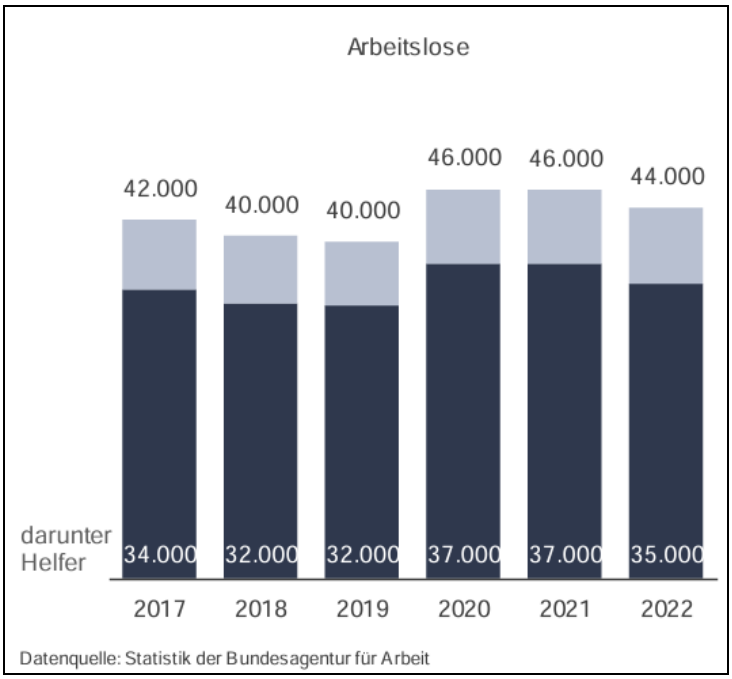


Abbildung 3:[20]

Berichte Blickpunkt Arbeitsmarkt Mai 2023 der Agentur für Arbeit:
„Im Jahresdurchschnitt 2022 waren 44.000 Pflegekräfte in Deutschland arbeitslos gemeldet, 2.000 weniger als im Vorjahr … Damit folgt die Arbeitslosigkeit, die im Zuge der Corona-Krise in den Jahren 2020 und 2021 auf das Niveau von 2015 gestiegen war, wieder dem längerfristig rückläufigen Trend. Auch wenn der Stand der Arbeitslosigkeit von vor der Corona-Krise noch nicht wieder erreicht ist.“[21]

[20] Siehe: https://statistik.arbeitsagentur.de; Arbeitslosenzahlen 2017 bis 2022

[21] Siehe: https://statistik.arbeitsagentur.de/DE/Statischer-Content/Statistiken/Themen-im-Fokus/Berufe/Generische-Publikationen/Altenpflege.pdf?__blob=publicationFile

Welche Rolle spielt die Resilienz der Bevölkerung für die Sicherheit von Kritischen Infrastrukturen?

Die Resilienz der Bevölkerung ist von entscheidender Rolle. Resilienz bezieht sich auf die Fähigkeit einer Gemeinschaft, sich von Schocks und Störungen zu erholen, sich anzupassen und gestärkt aus Krisen hervorzugehen. Diese Resilienz kann auf verschiedenen Ebenen existieren, einschließlich individueller, sozialer und institutioneller Aspekte.

1. Schnelle Erholung und Widerstandsfähigkeit:

Eine resiliente Bevölkerung ist besser in der Lage, sich schnell von Störungen zu erholen. Dies ist besonders wichtig, da eine schnelle Wiederherstellung nach Naturkatastrophen, Angriffen oder anderen Bedrohungen essentiell ist, um den normalen Betrieb aufrechtzuerhalten bzw. wieder neu zu starten.

2. Zusammenarbeit und Kommunikation:

Resiliente Gemeinschaften fördern Zusammenarbeit und effektive Kommunikation. Hier ist eine koordinierte Reaktion auf Notfälle entscheidend, und eine gut vernetzte Bevölkerung kann dazu beitragen, dass Informationen schnell und präzise weitergegeben werden.

3. Psychologische Belastbarkeit:

Es können psychologische Belastungen auftreten. Eine resiliente Bevölkerung verfügt über die Fähigkeit, mit Stress und Unsicherheit umzugehen. Psychologische Probleme wie Angst, Unsicherheit und Stress können die Fähigkeit der Menschen beeinträchtigen, angemessen auf Notfälle zu reagieren.

4. Selbsthilfe und Vorsorge:

Resiliente Gemeinschaften neigen dazu, besser auf mögliche Störungen vorbereitet zu sein. Dies kann die individuelle Vorsorge und Selbsthilfe einschließen, was insgesamt die Belastung auf Kritische Infrastrukturen reduziert.

Psychische Probleme in der Übersicht und ihre Folgen:

1. Angst und Panik:

In Zeiten von Krisen können Menschen Angst und Panik erleben, was ihre Fähigkeit beeinträchtigt, vernünftige Entscheidungen zu treffen.

2. Trauma:

Naturkatastrophen, Angriffe oder andere Zwischenfälle können traumatische Erfahrungen mit langfristigen psychischen Auswirkungen verursachen. Insbesondere bei Fällen der posttraumatischen Belastungsstörung kann sich die Notwendigkeit einer Psychotherapie ergeben.

3. Informationsüberlastung:

„Informationsflash“ über soziale Medien und Nachrichtenquellen kann zu Informations-überlastung führen, was wiederum zu Unsicherheit und Stress beiträgt. Hier muss auch die

teilweise reißerische Berichterstattung der Leitmedien erwähnt werden, da diese Art der Informationsweitergabe auch zu Extrembelastungen, gerade bei Personen mit niedriger Compliance, führen kann. Daher muss eine Filterung von Nachrichten in sämtlichen Medien (soweit dies durch breite Smartphone-Nutzung der Bevölkerung überhaupt möglich ist) durchgeführt werden. Nur sachliche und gezielte Informationen sollen der Bevölkerung mitgeteilt werden, um eine einigermaßen stabile Resilienz zu erhalten und keine Reizüberflutung zu verursachen.

4. Verlustängste:

Der Verlust von Eigentum, Arbeitsplätzen oder geliebten Menschen kann zu schweren emotionalen Belastungen führen.

Es ist wichtig, die psychologischen Aspekte bei der Entwicklung von Strategien zur Verbesserung der Resilienz zu berücksichtigen, um eine ganzheitliche Herangehensweise an die Sicherheit von Kritischen Infrastrukturen zu gewährleisten.

Mögliche Lösungen zur Förderung der psychischen Stabilität und somit auch der Resilienz:

4.1. Bildung und Sensibilisierung:

Öffentlichkeitsarbeit: Informationskampagnen können das Bewusstsein für potenzielle Risiken schärfen und die Bevölkerung darüber aufklären, wie sie sich vorbereiten können.

4.2. Schulungen und Übungen:
Diese können auf individueller und gemeinschaftlicher Ebene die Menschen darauf vorbereiten, angemessen auf Notsituationen zu reagieren. Katastrophenschutzübungen von Einsatzkräften sind wichtig. Warum wird bei solchen Übungen die breite Bevölkerung nicht mit eingeplant?

4.3. Notfallvorsorge und Selbsthilfe:
Individuelle Vorsorge: Förderung individueller Vorsorgepläne, einschließlich Notfallkits, Evakuierungsplänen und Kommunikationsstrategien.

Gemeinschaftliche Ressourcen: Gemeinschaften können Initiativen ergreifen, um gemeinschaftliche Ressourcen für den Notfall bereitzustellen, etwa Gemeinschaftsunterkünfte oder Nahrungsmittelvorräte.

4.4. Krisenkommunikation und -management:
Effektive Kommunikation: Sicherstellen, dass die Kommunikation in Krisensituationen klar, präzise und zeitnah erfolgt, um Verwirrung zu minimieren.

Notfallpläne: Notfallpläne entwickeln und regelmäßig aktualisieren, um auf verschiedene Arten von Störungen vorbereitet zu sein. Diese der Bevölkerung, soweit möglich, auch einmal jährlich (per Post/E-Mail) zukommen lassen.

4.5. Soziale Unterstützung und Gemeinschaftsbindung:
Förderung der Nachbarschaftshilfe: Entwicklung von Programmen zur Förderung der Nachbarschaftshilfe entwickeln, um sicherzustellen, dass Menschen in Krisenzeiten unterstützt werden (Beispiel: Bezirksebene der Städte).

4.6. Psychosoziale Unterstützung:
Bereitstellung von psychosozialer Unterstützung für Einzelpersonen und Gemeinschaften, um die Bewältigung von Stress und Traumata zu erleichtern.

Technologische Innovation zur Unterstützung:
Frühwarnsysteme: Implementierung von effektiven Frühwarnsystemen für Naturkatastrophen und Angriffe.

Digitale Plattformen: Nutzung von digitalen Plattformen und Technologien zur gezielten Informationsverbreitung und Koordination von Hilfsmaßnahmen.

Welche Erkenntnisse liegen im Rahmen der Risiko- und Krisenkommunikation in Richtung Bevölkerung vor? Hat die Pandemie diese Erkenntnisse beeinflusst und wenn ja, inwiefern? Welche Erkenntnisse gab es nach der Corona Pandemie und den nationalen Warntagen in Bezug auf die Risikokommunikation und -wahrnehmung?

- Die Risikokommunikation in der Coronazeit war unvollständig und teilweise von Falschinformationen geprägt. Bedauerlicherweise waren es vielfach Wissenschaftler und Akademiker, die – absichtlich oder unabsichtlich – Unzutreffendes behaupteten. Hier muss Aufklärung durch einen vom Bundestag eingesetzten Untersuchungsausschuss erfolgen.
- Dr. Karl Lauterbach postulierte ständig neue (Infektions-)Wellen, die entweder nicht eintrafen oder aber nicht derart verheerend waren, als dass dadurch die sogenannten 2- und 3G-Regeln, Ladenschließungen oder abendliche Ausgangssperren gerechtfertigt gewesen wären.
- Zur Vertiefung der Themenkomplexe Corona-Maßnahmenpolitik, Impfkampagnen sowie Risikokommunikation verweise ich gerne auf die Beiträge von:

  Prof. Mattias Desmet (Psychologe, Universität Gent, Belgien)[22], Gunnar Kaiser (Philosoph)[23], Dr. Josef Thoma (HNO-Arzt in Berlin), Dr. Michael Palmer (Biochemiker, lehrte an der University of Waterloo, Kanada)[24], Dr. Michael Yeadon (Pharmakologe, ehemals Forscher bei Pfizer), Dr. Denis G. Rancourt (Physiker, lehrte an der University of Ottawa)[25].
- Die Wahrnehmung vieler Bürger war,
  - dass die Lockdown-Maßnahmen nicht notwendig bis überzogen waren;
  - dass die Maßnahmen mit Mundschutz, Abstand, Besuchsverbot in Pflegeheimen und Krankenhäusern überzogen waren usw.

Es ist mittlerweile wissenschaftlich bestätigt, dass der Mundschutz nicht vor Ansteckung und Weitergabe des Virus geschützt hat. Es hat sich weiter bestätigt (Aussage von Janine Small, Pfizer, vor dem Corona-Ausschuss der EU), dass der Impfstoff nie vor Ansteckung oder Unterbindung der Weitergabe des Virus gedacht war. Er war nur für einen milderen Verlauf der Infektion vorgesehen. Von daher war die gesamte Kommunikation in Bezug auf die Impfung eine Täuschung am Bundesbürger. Betrachtet man die Akutschäden durch die

[22] „Psychologie von Corona - Massenpsychose und Massenformation (Mattias Desmet)“ (https://www.youtube.com/watch?v=IXnOYkkhqfg, 19.06.2022)
[23] „Warum Corona uns spaltet“ (https://www.youtube.com/watch?v=wkYplA9gl98, 19.12.2020)
[24] „Geimpft, geschädigt, geleugnet - Dr. Michael Palmer“ (https://www.youtube.com/watch?v=_IjVmw56zwA, 08.01.2024)
[25] „How Will History Treat The Coronavirus Lockdown? With Prof. Denis Rancourt“ (via „Ron Paul Liberty Report“, https://www.youtube.com/watch?v=awNrRiQCOdA, 28.04.2020)

Impfung, die Folgeschäden der Impfung[26] und auch die hohe Dunkelziffer von Schäden (nicht anerkannt, obwohl offensichtlich), so war die Risikokommunikation in den überwiegenden Fällen irreführend.

Ich verweise an dieser Stelle sowohl auf die Japanische Umverteilungsstudie[27] zum Covid-Impfstoff als auch auf die Evaluierungen von Großbritannien bei Geimpften während der Impfphasen – nach Alter gegliedert – und der damit verbundenen Mortalität.

Die Covid-Pandemie hat in der Bevölkerung nicht nur großes Unbehagen aufgrund der Grundrechtseinschnitte hervorgerufen, sondern auch gezeigt, dass die Bundesregierung durch Gesetzeserlasse im Rahmen der Notverordnung gegen die Freiheitsrechte der Menschen in Deutschland vorgegangen ist. Diese Maßnahmen waren überzogen und dürfen sich nie wieder wiederholen.

Egal wie stark ausgeprägt eine Krise ist: Ein gesundes Maß an Sicherheit und Menschenverstand ist einzuhalten. Korruption und „Vetternwirtschaft“ ist durch verschärfte Gesetzgebung mit Androhung hoher Freiheitsstrafen präventiv einzudämmen. Es bedarf eines ständigen Aufsichtsgremiums im Landtag, welches sich auf Korruption und Lobbyisten-einfluss auf Politiker spezialisiert. Dadurch wird dem Missbrauch von Steuergeldern in einer Krisenlage vorgebeugt. Gemäß dem Motto „Die Katze lässt das Mausen nicht!“ dürfte jedoch klar sein: Korruption und Betrug können niemals vollständig unterbunden werden.

Wo lagen aus Ihrer Sicht Probleme in der Krisenkommunikation?

Die Krisenkommunikation während der Covid-19-Pandemie war eine komplexe Herausforderung mit verschiedensten Problemen.

Uneinheitliche und inkonsistente Informationen:

Verbreitung uneinheitlicher und widersprüchlicher Informationen von verschiedenen Quellen, einschließlich unterschiedlicher Aussagen von Regierung, Gesundheitsbehörden und Medien. Dies führte zu Verwirrung und Unsicherheit in der Bevölkerung.

Mangelnde Transparenz und Kommunikationsschwierigkeiten:

In einigen Fällen wurde der Mangel an Transparenz in Bezug auf die Verfügbarkeit von Ressourcen, Testkapazitäten und anderen wichtigen Informationen kritisiert.

Fehlende Koordination zwischen Staaten der EU:

Auf internationaler Ebene gab es oft eine mangelnde Koordination und Zusammenarbeit zwischen Ländern bei der Bekämpfung der Pandemie. Dies betraf sowohl den Austausch von Informationen als auch die gemeinsame Entwicklung und Umsetzung von Strategien.

Wissenschaftliche Unsicherheit:

Es war schwierig, klare und konsistente Botschaften zu vermitteln, insbesondere wenn wissenschaftliche Erkenntnisse sich im Laufe der Zeit änderten. Die Verbreitung von

[26] Siehe: https://ijvtpr.com/index.php/IJVTPR/article/view/23

[27] Siehe: https://web.archive.org/web/20210611193138/https://www.pmda.go.jp/drugs/2021/P20210212001/672212000_30300AMX00231_I100_1.pdf

Missinformationen und Desinformationen über das Virus, seine Herkunft, mögliche Behandlungen und Präventionsmaßnahmen waren ein erhebliches Problem.

Kommunikation von notwendigen Maßnahmen, wie Lockdowns, sozialer Distanzierung und Maskenpflicht, stieß auf Widerstand und Verwirrung in der Bevölkerung. Die Gründe hierfür waren vielfältig, darunter mangelnde Sachinformation und Falschdarstellungen. Auch gab es unterschiedliche Umsetzung auf regionaler Ebene, sodass dies weitere Fragen und Zweifel in der Bevölkerung aufkommen ließ.

Die psychischen Auswirkungen der Pandemie wurden nicht ausreichend betont. Die Herausforderungen im Zusammenhang mit sozialer Isolation, Ängsten und Unsicherheiten erforderten eine umfassende Herangehensweise, einschließlich psychologischer Unterstützung und entsprechender Kommunikation. Hier sind im Nachhinein eklatante Defizite zu erkennen, welche zukünftig nicht mehr vorkommen dürfen.

Fazit:
In Nachbetrachtung der SARS-CoV-2-Pandemie ist die Bedeutung klarer, konsistenter, transparenter und koordinierter Krisenkommunikation enorm wichtig. Die Integration von wissenschaftlich fundierten Informationen, klaren Handlungsanweisungen und einem Verständnis für die psychologischen Bedürfnisse der Bevölkerung ist entscheidend, um Vertrauen aufzubauen. Nur so kann eine wirksame Reaktion auf zukünftige Pandemien gewährleistet werden.

Zusammenfassend werden folgende Fragen beantwortet:

Inwieweit beeinträchtigen Fake News die Arbeit der Kritischen Infrastrukturen?

Inwieweit beeinträchtigen Desinformationskampagnen die Arbeit der Kritischen Infrastrukturen?

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 Auswirkung davon sein?

Welche Maßnahmen empfehlen Sie hier konkret? Welche Akteure sehen Sie hier insbesondere in der Pflicht?

Fake News können die Arbeit von Kritischen Infrastrukturen auf verschiedene Weisen beeinträchtigen:

- Falsche Informationen über Naturkatastrophen, Angriffe oder andere Notfälle können Verwirrung stiften und zu falschen Entscheidungen führen. Kritische Infrastrukturen und Rettungsdienste könnten aufgrund von irreführenden Informationen Schwierigkeiten haben, angemessen zu reagieren.
- Verbreitung von Falschinformationen über Warnsysteme kann das Vertrauen der Bevölkerung in diese Systeme untergraben. Dies könnte dazu führen, dass Menschen legitime Warnungen ignorieren, was die Wirksamkeit von Evakuierungs-

und Schutzmaßnahmen beeinträchtigt. Auch könnten falsche Bedrohungen oder Gefahren gemeldet werden, was zu unnötiger Panik und öffentlichen Unruhen führen kann. Dies könnte die Sicherheit von Menschen gefährden und die Fähigkeit der Kritischen Infrastrukturen beeinträchtigen, einen geordneten Notfallplan umzusetzen.

- Fake News können sich auch auf die Kommunikationssysteme auswirken, die für die Koordination von Rettungsdiensten und anderen Einheiten unerlässlich sind. Falsche Informationen könnten dazu führen, dass Teams ineffektiv arbeiten oder Ressourcen falsch verteilen.
- Kritische Infrastrukturen, die stark von digitalen Systemen abhängig sind, könnten durch gezielte Cyberangriffe beeinträchtigt werden. Fake News, die als Teil von Desinformationskampagnen verbreitet werden, könnten als Tarnung für Cyberangriffe dienen.
- Fake News können politisch motiviert sein und darauf abzielen, das Vertrauen in die Landesregierung oder kritische Institutionen zu untergraben. Dies könnte zu politischer Instabilität führen und die Zusammenarbeit zwischen Behörden und der Bevölkerung beeinträchtigen. Auch kann es zu Widerständen durch direkte Angriffe von Mobs kommen oder es entstehen Demonstrationen, die wiederum eine Gefahr der Kritischen Infrastruktur darstellen. Auch werden durch solche Aktionen durch die Bevölkerung Einsatzkräfte gebunden, die an anderer Stelle benötigt werden, um die ursächliche Krise zu bewältigen.

Um die Auswirkungen von Fake News auf die Arbeit Kritischer Infrastrukturen zu minimieren, sollen nun verschiedene Maßnahmen vorgeschlagen werden:

Schulung der Bevölkerung:

Programme zur Förderung von Medienkompetenz und kritischem Denken, um Menschen zu befähigen, Falschinformationen zu erkennen und zu vermeiden. Gezielte Aufklärungskampagnen, welche die Öffentlichkeit über die Auswirkungen von Fake News auf die öffentliche Sicherheit informieren.

Klare und genaue Kommunikation:

Kritische Infrastrukturen sollten klare, genaue und regelmäßige Informationen bereitstellen, insbesondere in Notfällen. Institutionen sollten soziale Medien und andere digitale Plattformen nutzen, um direkte, authentische Informationen zu verbreiten und so Falschinformationen zu kontern. Die Landesregierung muss sicherstellen, dass verantwortungsvoll und ethisch berichtet wird. Falls notwendig: Sondergesetze und Erlasse, welche ausschließlich auf die vorhandene Krise und zeitlich klar beschränkt sind.

Automatisierte Erkennung von Falschinformationen:

Technologische Lösungen, wie Algorithmen zur automatisierten Erkennung von Falschinformationen, können dazu beitragen, die Verbreitung von Fake News einzudämmen. Herstellen der Transparenz bei den Algorithmen von sozialen Medien, um sicherzustellen, dass Benutzer besser verstehen, wie Inhalte priorisiert und angezeigt werden. Außerdem sollte eine internationale Zusammenarbeit zwischen Regierungen, Medien und Technologieunternehmen angestrebt werden, um gemeinsam gegen globale Desinformationskampagnen vorzugehen. Entwicklung von Standards und „Best Practices“ für digitale Plattformen, um die Verbreitung von Falschinformationen zu minimieren.

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

Ich möchte an dieser Stelle erneut auf die Gefahren von Cyber-Angriffen hinweisen – ganz besonders unser Gesundheitssystem betreffend.

Mit der zunehmenden Vernetzung von Einrichtungen im Gesundheitswesen stellt sich für die einzelne Praxis oder das einzelne Krankenhaus nicht mehr die Frage, ob man angegriffen wird – sondern wann. Daher ist es wichtig rechtzeitig vorzusorgen.

Fakt ist: Die Lage der Cybersicherheit ist angespannt und wird sich angesichts zunehmend professioneller Hackerangriffe künftig auch weiter zuspitzen. Zumindest geht dies aus dem in 2023 vorgestellten Bericht zur Lage der IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervor.[28] Das BSI beobachtet nicht nur Cyberangriffe mit Ransomware bei großen, zahlungskräftigen Unternehmen, sondern auch bei kleinen und mittleren Organisationen sowie staatlichen Institutionen und Kommunen.

Auch in Praxen und Kliniken sind mehr und mehr Prozesse von einer funktionierenden digitalen Infrastruktur abhängig und somit Angriffsfläche von Cyberkriminalität. Diese wird nicht nur durch gezielte Angriffe gefährdet, sondern auch durch Kollateralschäden bei Angriffen und Malware, die nicht ursprünglich auf Einrichtungen des Gesundheitswesens zielten. Die Resultate sind die gleichen: eine Gefährdung der Patientenversorgung und der wirtschaftlichen Situation der Einrichtung.

Der IT-Konzern IBM berichtet in seinem Security X-Force Threat Intelligence Index 2023[29], dass Ransomware eine der wichtigsten Arten von Schadsoftware weltweit ist. Bei einem Befall mit Ransomware werden alle erreichbaren Programme und Daten des Opfers verschlüsselt. Diese Schadsoftware ist auch als Verschlüsselungstrojaner bekannt. Es erfolgt dann durch den Versender eine Aufforderung, ein Lösegeld zu zahlen, um den Schlüssel zur Entschlüsselung der Daten zu erhalten.

Die perfekte Sicherheit gibt es nicht. Aufgabe ist es, mit technischen und organisatorischen Maßnahmen das Eintrittsrisiko eines Vorfalls zu mindern und die Auswirkungen eines möglichen Angriffes zu mildern.

Wird versäumt, technische Vorkehrungen zu treffen, um sich vor Schadsoftware und anderen Cyberangriffen zu schützen, so ist die Wiederherstellung von Daten, IT-Systemen und die Rückgewinnung des Vertrauens der Patienten die kleinere Sorge. Die größere Sorge ist die Verantwortung vor Gericht. Das zeigt das Beispiel einer deutschen Hilfsorganisation, die nach einem Cyberangriff ein Bußgeld in Höhe von 10.000 Euro zahlen musste[30] sowie das Beispiel der Gesundheitsbehörde in Neapel mit 30.000 Euro Bußgeld, weil sie Art. 5, 25 und 32 der DSGVO verletzt hatte.[31] In beiden Fällen verschafften die Hacker sich Zugriff zu sensiblen personenbezogenen Daten.

Die technische Infrastruktur in Krankenhäusern ist mittlerweile sehr komplex geworden und es bedarf sehr viel personellen und finanziellen Aufwands, um diese stark heterogenen Systeme abzusichern. Vor allem steht das Risiko eines Ausfalls telemedizinischer Angebote von Kliniken im Raum, die bei einem Ausfall sogar ganze Abteilungen nicht belegen können (Beispiel: Stroke Unit).

---

[28] Siehe: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

[29] Siehe: https://www.ibm.com/reports/threat-intelligence

[30] Siehe: https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-hilfsorganisation-2022-12-31-DE-2828.php

[31] Siehe: https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-mednow-medical-2023-10-13-IT-3216.php

Maßnahmen zur Prävention:

- Regelmäßige Updates aller Systeme, dadurch Schließung auch neu bekannt gewordener Sicherheitslücken.
- Aktuelle Firewall und Antivirensoftware: Sie müssen aktuell und ausreichend streng sein, um Angriffe von außen abzuhalten. Aber: Einstellungen dürfen nicht so einschränkend sein, dass sie die tägliche PC-Arbeit der Mitarbeiter behindern, denn dann besteht das Risiko, dass Mitarbeiter Wege finden, die „lästigen" Sicherheitsvorkehrungen zu deaktivieren oder auf anderem Wege zu umgehen.
- Vorgaben zu Passwörtern und Umgang mit Zugangsdaten: Verwendung sicherer Passwörter – oder besser: Passsätze – sowie gegebenenfalls eines Passwortmanagers. Auch die vielerorts noch praktizierte Weitergabe von Zugangsdaten an Praktikanten oder Studenten, die nur vorübergehend mit dem System arbeiten, ist gefährlich und sollte unterbunden werden.
- Investitionsverpflichtungen des Bundeslandes NRW zügig umsetzen und kurze Antragswege schaffen sowie evtl. vorhandene Bürokratiehürden abschaffen.
- Sensibilisierung von Mitarbeitern hinsichtlich Phishing und anderer verdächtiger Phänomene: Woran ist eine verdächtige E-Mail zu erkennen? Was, wenn ein angeblich neuer Mitarbeiter der IT am Telefon ist und nach Zugangsdaten fragt?
- Gute Fehlerkultur: Sollten Angestellte doch einmal auf einen verdächtigen Link geklickt haben, sollten sie sich nicht dazu verleitet fühlen, den Vorfall aus Angst vor Konsequenzen zu vertuschen.

****

Anlage und weiterführende Informationen zu KRITIS außerhalb des Fragenkataloges:

1) Aufschlüsselung betroffener Bereiche der KRITIS

Sektor Energie

- Strom, Gas, Kraftstoffversorgung (inklusive Logistik);
- insbesondere Einrichtungen zur Entstörung und Aufrechterhaltung der Netze

Sektor Wasser, Entsorgung

- Hoheitliche und privatrechtliche Wasserversorgung
- insbesondere Einrichtungen zur Entstörung und Aufrechterhaltung der Netze

Sektor Ernährung, Hygiene

- Produktion, Groß- und Einzelhandel (inklusive Zulieferung, Logistik)

Sektor Informationstechnik und Telekommunikation

- insbesondere Einrichtungen zur Entstörung und Aufrechterhaltung der Netze

Sektor Gesundheit

- insbesondere Krankenhäuser, Rettungsdienst, Pflege, niedergelassener Bereich, Medizinprodukthersteller, Arzneimittelhersteller, Apotheken, Labore

Sektor Finanz- und Wirtschaftswesen

- insbesondere Kreditversorgung der Unternehmen, Bargeldversorgung, Sozialtransfers

- Personal der Bundesagentur für Arbeit und Jobcenter zur Aufrechterhaltung des Dienstbetriebes (insbesondere Auszahlung des Kurzarbeitergeldes)

Sektor Transport und Verkehr

- insbesondere Betrieb für Kritische Infrastrukturen, öffentlicher Personennah- und Personenfern- und Güterverkehr

- Personal der Deutschen Bahn und nicht bundeseigener Eisenbahnen zur Aufrechterhaltung des Dienstbetriebes

- Personal zur Aufrechterhaltung des Flug- und Schiffsverkehrs

Sektor Medien

- insbesondere Nachrichten- und Informationswesen sowie Risiko- und Krisenkommunikation

Sektor staatliche Verwaltung (Bund, Land, Kommune)

- Kernaufgaben der öffentlichen Verwaltung und Justiz, Polizei, Feuerwehr, Katastrophenschutz, Justizvollzug, Veterinärwesen, Lebensmittelkontrolle, Asyl- und Flüchtlingswesen einschließlich Abschiebungshaft, Verfassungsschutz, aufsichtliche Aufgaben sowie Hochschulen und sonstige wissenschaftlichen Einrichtungen, soweit sie für den Betrieb von sicherheitsrelevanten Einrichtungen oder unverzichtbaren Aufgaben zuständig sind

- Gesetzgebung/Parlament

Sektor Schulen, Kinder- und Jugendhilfe, Behindertenhilfe

- Sicherstellung notwendiger Betreuung in Schulen, Kindertageseinrichtungen, Kindertagespflege, stationären Einrichtungen der Kinder- und Jugendhilfe und Einrichtungen für Menschen mit Behinderung

2) Einsatzplanung und Bewältigung von Schadensereignissen mit einer größeren Anzahl Verletzter oder Erkrankter – MANV (Massenanfall von Verletzten oder Erkrankten)

Ein Massenanfall von Verletzten oder Erkrankten im Sinne der nachfolgenden Hinweise liegt vor, wenn ein Großschadensfall oder eine Katastrophe mit einer größeren Anzahl von Verletzten oder Erkrankten gegeben ist (siehe Landeskatastrophenschutzgesetz NRW).

„Ein **Großschadensfall** ist gekennzeichnet durch eine Vielzahl von Verletzten oder Erkrankten bei häufig nicht mehr funktionsfähiger oder nicht mehr ausreichender Infrastruktur am Schadensort, teilweise auch durch das Bestehen einer erheblichen Gefährdung der Einsatzkräfte im Bereich des Schadensereignisses. Dabei ist davon auszugehen, dass ein Missverhältnis zwischen dem Bedarf an der Schadensstelle und der Kapazität des Rettungsdienstes entsteht, so dass – zumindest für einen gewissen Zeitraum – nicht mehr

nach den Kriterien der individuellen medizinischen Versorgung verfahren werden kann.“ (DIN 13050:2015-04, Begriffe im Rettungswesen)

Eine **Katastrophe** ist ein Geschehen, das Leben oder Gesundheit zahlreicher Menschen, die Umwelt, erhebliche Sachwerte oder die lebensnotwendige Versorgung der Bevölkerung in so ungewöhnlichem Maße gefährdet oder schädigt, dass es geboten erscheint, ein zu seiner Abwehr und Bekämpfung erforderliches Zusammenwirken von Behörden, Stellen und Organisationen unter die einheitliche Leitung der Katastrophenschutzbehörde zu stellen.

Die Hinweise konkretisieren die sich aus dem Feuerwehrgesetz (FwG), Polizeigesetz (PolG), Rettungsdienstgesetz (RDG) und Landeskatastrophenschutzgesetz (LKatSG) ergebenden Bestimmungen. Die Zuständigkeiten nach diesen Gesetzen bleiben unberührt. Alle Stellen und Behörden, die zur Hilfeleistung herangezogen werden können, sind aufgerufen, die erforderliche Vorsorge zu treffen.

Oberstes Ziel bei der Bewältigung eines MANV ist, den anfänglichen Mangel an Ressourcen so zu organisieren und zu verwalten, dass eine fachgerechte Versorgung aller betroffenen Patienten nach den individualmedizinischen Kriterien des Rettungsdienstes so schnell wie möglich wieder hergestellt wird. Um das Missverhältnis zwischen dem Versorgungsbedarf und den zur Verfügung stehenden medizinischen Möglichkeiten möglichst schnell zu beseitigen, ist es erforderlich, unverzüglich zusätzliches Fachpersonal und medizinisches Material zum Notfallort zu bringen und dort eine Basis-Infrastruktur herzustellen, die eine medizinische Versorgung zulässt. Weiterhin ist es bis zur Wiederherstellung der medizinischen Regelversorgung notwendig, die Versorgung der einzelnen Patienten konsequent an der Dringlichkeit der jeweiligen Gesundheitsstörungen auszurichten (Sichtung), um durch die optimale Nutzung der zur Verfügung stehenden Kapazitäten das Überleben möglichst vieler Betroffenen zu sichern. Ferner ist die konsequente Umsetzung der Planungen für einen MANV geboten. Sofern nach der Sichtung eine stationäre Behandlung erforderlich ist, sind Verletzte und Erkrankte durch die gezielte Zuweisung in geeignete Krankenhäuser möglichst frühzeitig einer individualmedizinisch-klinischen Versorgung zuzuführen.[32]

„Die zur Bewältigung einer Schadenslage benötigten Ressourcen sind in einem stufenförmig aufwachsenden Wellenkonzept darzustellen (…). Die unteren Katastrophenschutzbehörden sind gehalten, in den Planungen anhand von Verletztenzahlen unter Berücksichtigung der örtlichen Gegebenheiten und der vorhandenen personellen und materiellen Ressourcen zu definieren, ab welcher Größenordnung eines Schadensereignisses Ressourcen der nächsten Welle benötigt werden.“[33]

Planungsgrundlage:
„Als Planungsgrundlage wird ein punktuelles oder kleinflächiges Schadensereignis mit einer Vielzahl von Verletzten oder Erkrankten angesetzt. Dieses Schadensereignis ist in der Frühphase durch einen Ressourcenmangel (personell wie materiell) gekennzeichnet, in der Spätphase durch eine Vielzahl zu koordinierender Ressourcen.

Beim Ressourcenmangel sind folgende Aufgaben vorrangig zu bewältigen:

- Priorisierung der Aufgaben (Sichtung der Patienten)
- Bündelung der Aufgaben und Ressourcen (Konzentration)
- Pufferung aufschiebbarer Aufgaben (Transportorganisation und Verteilung der Patienten auf die Krankenhäuser)

[32] Vgl. „Konzeption des Ministeriums für Inneres, Digitalisierung und Migration für die Einsatzplanung und Bewältigung eines Massenanfalls von Verletzten (ManV-Konzept)“ (01.08.2016, https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf)
[33] Ebenda.

- Einbindung der Krankenhäuser

Es werden folgende Festlegungen getroffen: Prozentuale Verteilung der Verletzungsgrade bei einem punktuellem Schadensereignis:

Verletzungsgrad	Prozentualer Anteil bezogen auf alle Verletzten
akut vital bedroht	40
schwerverletzt	20
leichtverletzt	40

Kategorisierung der Verletzungsgrade:

Kategorie		Verletzungsgrad	Erforderliche Maßnahmen
	I	akut vital bedroht	Sofortbehandlung
	II	schwerverletzt	dringende Behandlung
	III	leichtverletzt	spätere (ambulante) Behandlung
	IV	ohne Überlebenschance	betreuende (abwartende) Behandlung
		Tote	Registrierung

"[34]

„Die zur Bewältigung einer Schadenslage benötigten Ressourcen sind in einem stufenförmig aufwachsenden Wellenkonzept dargestellt. Den einzelnen Wellen wird dabei bewusst keine Verletztenzahl zugeordnet, da die Bewältigung eines Schadensereignisses maßgeblich von den örtlichen Gegebenheiten vor allem dem vorhandenen Personal und Material abhängt (Unterschied: Großstadt - ländlicher Raum). Die unteren Katastrophenschutzbehörden sind daher gehalten, in Abstimmung mit den jeweiligen Trägern des KatS- und Rettungsdienstes ihre Planungen zu definieren, ab welcher Größenordnung eines Schadensereignisses Ressourcen der nächsten Welle benötigt werden.

1. Welle:
Hilfeleistung für individuelle Notfälle. Regelversorgung auf örtlicher Ebene. Notwendiges Personal und Gerät: - Regelvorhaltung im Rettungsdienst laut Bereichsplan - ggf. einsatzbereite Regelvorhaltung im Rettungsdienst der Nachbarbereiche (siehe RDG) - ggf. Reservefahrzeuge des eigenen Bereichs und der Nachbarbereiche.

2. Welle:
Hilfeleistung für Schadensereignisse mit einer Vielzahl von Verletzten oder Erkrankten, deren Bewältigung neben den Ressourcen der 1. Welle weiterer Unterstützung bedarf.

Standardisierter flächendeckender Grundschutz. Ggf. sind Patientenablagen ein zurichten und der Aufbau und Betrieb von Behandlungsplätzen notwendig.

[34] „Konzeption des Ministeriums für Inneres, Digitalisierung und Migration für die Einsatzplanung und Bewältigung eines Massenanfalls von Verletzten (ManV-Konzept)" (01.08.2016, https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf)

Notwendiges Personal und Gerät:

- Personal und Gerät der 1. Welle - zusätzlich SEGen
- ggf. Katastrophenschutz-Einsatzeinheiten und/oder einzelne Leistungsmodule) aus dem eigenen Bereich
- ggf. Unterstützung durch Feuerwehr und / oder THW.

3. Welle:

Hilfeleistungen für Schadensereignisse mit einer Vielzahl von Verletzten oder Erkrankten, die nicht mit dem Potenzial des Grundschutzes abzudecken sind. Der Einsatz von zusätzlichen Katastrophenschutz-Einsatzeinheiten aus den Nachbarkreisen ist notwendig.

Die Versorgung der Patienten erfolgt nach den Grundsätzen der Mangelverwaltung. Patientenablagen sind einzurichten und der Aufbau und Betrieb von Behandlungsplätzen ist notwendig.

Notwendiges Personal und Gerät:

- Personal und Gerät der 1. und 2. Welle
- Katastrophenschutz-Einsatzeinheiten und/oder Leistungsmodule aus benachbarten Bereichen – Feuerwehr
- ggf. THW.

4. Welle:

Hilfeleistung für Schadensereignisse mit einer Vielzahl von Verletzten oder Erkrankten, die nicht mit dem Potenzial der 3. Welle bewältigt werden können. Zusätzlich ist die Infrastruktur zerstört und/oder Personen sind kontaminiert. Die Versorgung der Patienten erfolgt nach den Grundsätzen der Mangelverwaltung. Ggf. ist der Aufbau und Betrieb von Behandlungsplätzen mit der Möglichkeit zur Dekontamination Verletzter notwendig.

Notwendiges Personal und Gerät:

- Personal und Gerät der 1. bis 3. Welle
- ggf. Einsatz Medizinische Task-Forces (MTF)
- aus benachbarten Bundesländern (2)
- ggf. Unterstützung durch die Bundeswehr im Rahmen der zivil-militärischen Zusammenarbeit.

Leistungen koordinieren und gezielt einsetzen

Ein Schadensereignis mit einer Vielzahl von Verletzten oder Erkrankten ist – bei entsprechendem Ausmaß – nicht mehr alleine mit den Ressourcen eines Landkreises zu beherrschen. Da die bisherigen regionalen oder organisationseigenen Konzepte zur überörtlichen Hilfeleistung untereinander nur eingeschränkt kompatibel sind, ist zur effektiven Abarbeitung von komplexen Schadenslagen eine Standardisierung von Leistungen erforderlich. Ziel ist, im Ereignisfall gezielt die fehlenden Leistungen landesweit anzufordern und Einsatzkräfte aus anderen Kreisen in die bereits an der Einsatzstelle bestehenden Strukturen einzubinden."[35]

[35] „Konzeption des Ministeriums für Inneres, Digitalisierung und Migration für die Einsatzplanung und Bewältigung eines Massenanfalls von Verletzten (ManV-Konzept)" (01.08.2016, https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf)

Schadensparameter in der Übersicht:[36]

Schutzgut	Schadensparameter	Benötigte Informationen z.B.	Mögliche Informationsquellen (Behörden der Ebene Kommune, Land und Bund) z.B.
Mensch	• Tote • Verletzte • Hilfebedürftige	• Einwohnerzahl • Einwohnerdichte • Anzahl der Haushalte • Ein- u. Auspendler • Touristen • Verkehrswege (Straße, Schiene) • Versorgungsnetze (Strom, Gas, Wasser)	• Statistische Ämter • Einwohnermeldeämter • Tourismusinformation • Planungs- u. Verkehrsämter • Bundesinstitut für Bau-, Stadt- und Raumforschung • Stadtwerke, Regionalversorger, Netzbetreiber, Wasserverbände
Umwelt	• Geschützte Gebiete • Landwirtschaftliche Nutzfläche • Waldflächen • Nutzvieh	• Flächen • Tierbestand (GVE oder Anzahl)	• Statistische Ämter • Umweltämter • Amt für Land- und Forstwirtschaft • Bundesamt für Naturschutz • Landwirtschaftskammer
Volkswirtschaft	• Wirtschaftliche Schäden der Öffentlichen Hand • Wirtschaftliche Schäden der Privaten Wirtschaft • Wirtschaftliche Schäden der Privaten Haushalte	• Zahlen der Doppik (Bilanz – Anlagevermögen) • Haushalt (Investitionen) • Gewerbesteuereinnahmen • Arbeitsplätze in betroffenen Unternehmen	• Ämter für Wirtschaft • Ämter für Finanzen • Ämter für Kreis- u. Regionalentwicklung • Industrie- u. Handelskammer
Immateriell	• Folgen für die Öffentliche Sicherheit und Ordnung • Psychologische Auswirkungen bei der Bevölkerung • Auswirkung für die Politik • Schäden an Kulturgütern	• Einsatzzahlen der Einsatzkräfte • Einschätzung der Folgen durch Experten • Einschätzung des Drucks der Öffentlichkeit/Medien auf die politische Führung • Anzahl/Standorte des unbeweglichen und beweglichen Kulturgutes	• Leitstelle(n) • Führung von FW, Polizei, Pressestellen • Denkmalschutzbehörden

[36] Quelle: https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf

Einsatzeinheit-Erstversorgung

Leistungsmodul Führung

Leistungsmodul Erstversorgung (entspricht SEG-Erstversorgung)

Leistungsmodul Transport

Leistungsmodul Betreuung und Logistik

Leistungsmodul Technik und Sicherheit

Einsatzeinheit-Behandlung

Leistungsmodul Führung

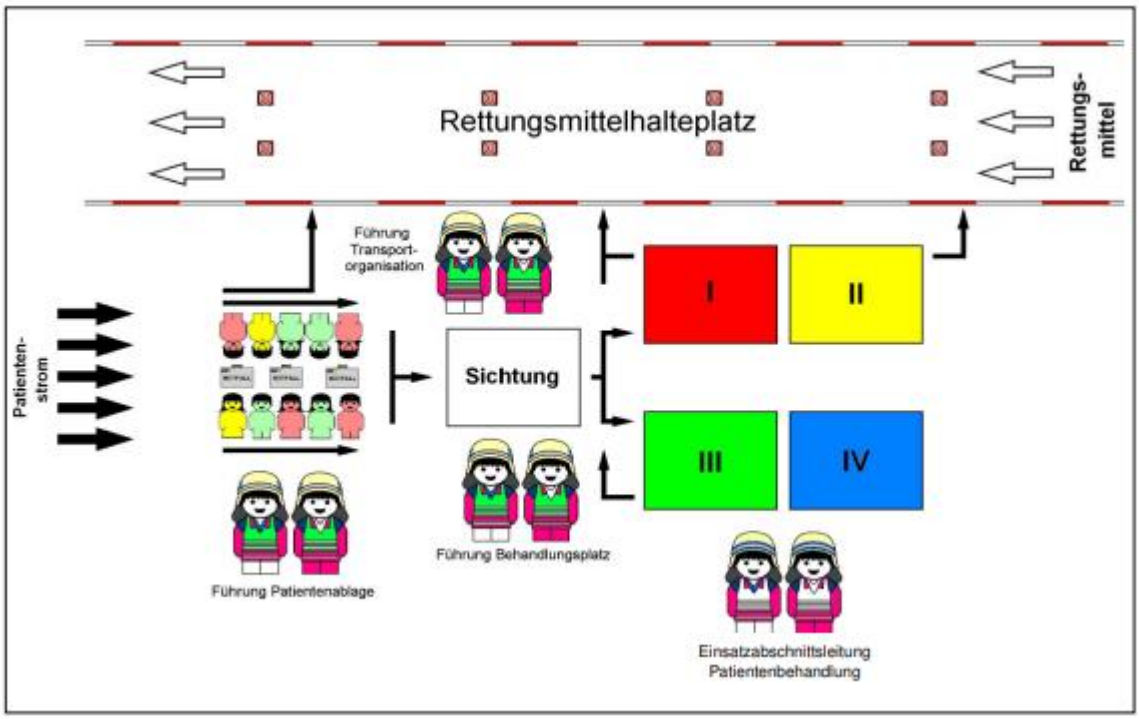
Leistungsmodul Behandlung

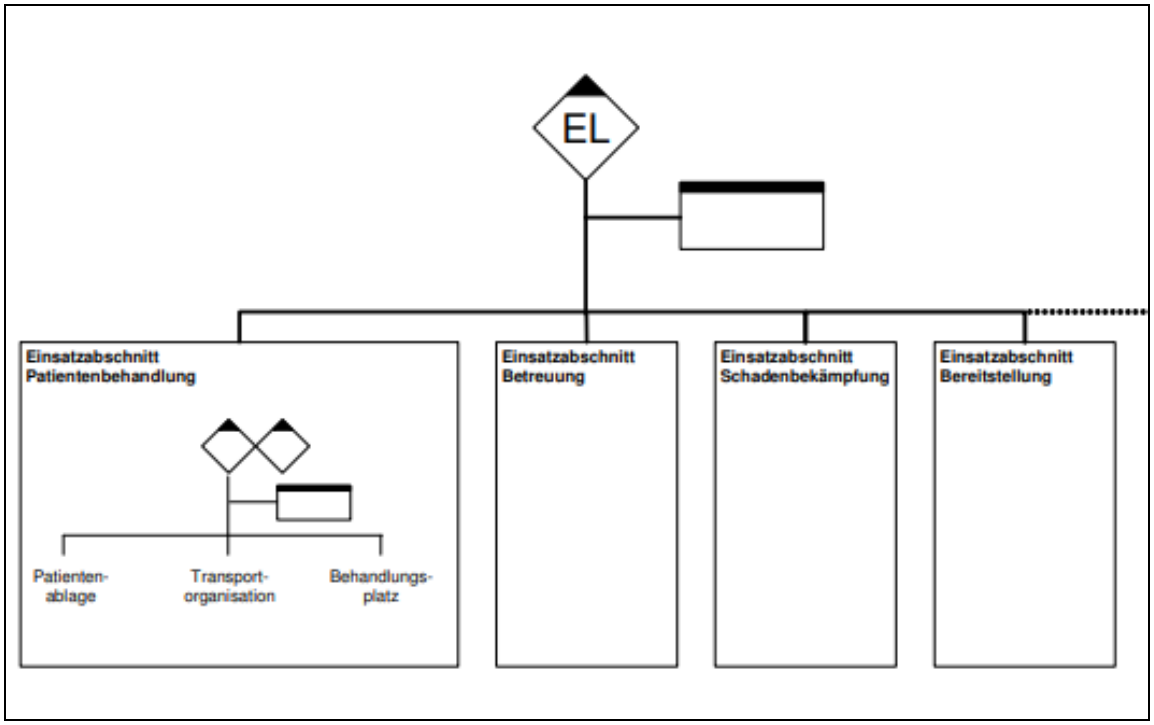
Leistungsmodul Transport

Leistungsmodul Betreuung und Logistik

Leistungsmodul Technik und Sicherheit

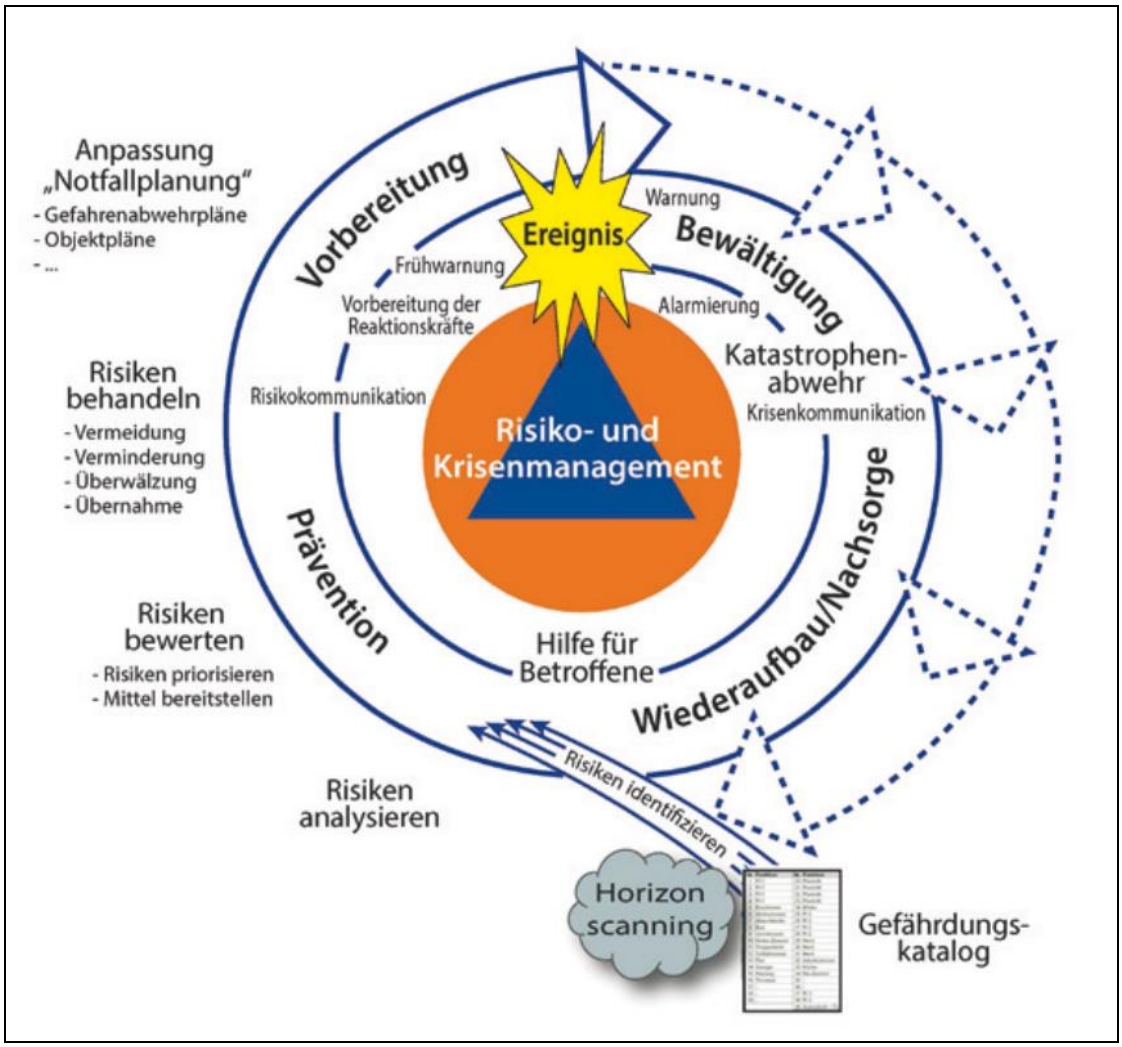
Obige Abbildungen: Quelle: https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf





Obige Abbildungen: Quelle: https://www.lfs-bw.de/fileadmin/LFS-BW/themen/einsatzdienst/sonderlagen/dokumente/ManV_Konzept_2016.pdf

Schaubild: Ablaufplan eines Ereignisses (Quelle: Deutscher Bundestag Drucksache 19/9520, 19. Wahlperiode)**:**



Weitere Informationen rund um die Risikoanalyse im Bevölkerungsschutz entnehmen Sie bitte dem „Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz" des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe – Band 16. Für die eigene Nutzung bearbeitbare Dokumentvorlagen schauen Sie bitte unter: www.bbk.bund.de/risikoanalyse nach.

Die psychosoziale Notfallversorgung der Bevölkerung

Die Psychosoziale Notfallversorgung (PSNV) umfasst die psychologische, soziale, administrative und seelsorgliche Hilfe für von Notfällen Betroffene (Opfer, Angehörige, Einsatzkräfte). Zur Sicherstellung der seelsorgerischen Betreuung bei Katastrophen und schweren Unglücksfällen haben das Land Baden-Württemberg – vertreten durch das Innenministerium – und die Evangelischen Landeskirchen Baden und Württemberg die Diözese Rottenburg-Stuttgart sowie die Erzdiözese Freiburg im Dezember 2006 eine Vereinbarung getroffen. Nach dieser Vereinbarung benennen die Kirchen den unteren Katastrophenschutzbehörden speziell für Katastrophenfälle ausgebildete Notfallseelsorger, welche bei ihren Einsätzen Helferstatus genießen. In den Stadt- und Landkreisen sind vergleichbare Vereinbarungen zu treffen, um die Zusammenarbeit mit der Notfallseelsorge zu sichern. Betroffene können nach einem Unglück auch von den sogenannten Kriseninter-

ventionsteams und Notfallpsychologen Hilfe erhalten. In Krisenberaterteams, die bei den vier Landespolizeidirektionen, beim Polizeipräsidium Stuttgart und bei der Bereitschaftspolizei eingerichtet sind, wirken neben Polizei-Ärzten auch haupt- oder nebenberufliche Polizei-Seelsorger mit. Die Hilfsorganisationen bilden Fachkräfte für die psychosoziale Nachsorge ihrer Einsatzkräfte und die psychologische, soziale und seelsorgerische Hilfe von Betroffenen aus und halten Teams für einen MANV (Massenanfall von Verletzten) vor. Die örtlichen Maßnahmen der PSNV werden im Einsatzabschnitt „Betreuung“ zusammengefasst und koordiniert. Lageabhängig können die Maßnahmen der „Betreuung“ einschließlich PSNV auch dem Einsatzabschnitt „Patientenbehandlung“ unterstellt werden. Übergeordnete Aufgaben, wie beispielsweise die Einrichtung eines Sorgentelefons, sollen vom Führungsstab, soweit eingerichtet vom Verwaltungsstab, übernommen werden.

Atomare Ereignisse:

„Nach dem Ende des Kalten Krieges und dem Wegfall der damaligen bipolaren Bedrohungslage im vergangenen Jahrhundert wurden jedoch Vorhaltungen auf diesem Sektor reduziert oder aufgelöst. Die deutliche Veränderung der internationalen sicherheitspolitischen Situation in diesem Jahrhundert führt nun aber wieder dazu, dass auch die staatliche Notfallvorsorge, sowie die zivile Verteidigung einschließlich des Zivilschutzes fortentwickelt und an die heutigen Bedrohungslagen angepasst werden müssen. Im neuen „Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ schreibt Bundeskanzlerin Angela Merkel: „Die Welt im Jahr 2016 ist eine Welt in Unruhe. Auch in Deutschland und Europa spüren wir die Folgen von Unfreiheit, Krisen und Konflikten in der unmittelbaren Nachbarschaft unseres Kontinents. Wir erleben zudem, dass selbst in Europa Frieden und Stabilität keine Selbstverständlichkeit sind …“ Im Zusammenhang mit den Erfordernissen einer gesamtgesellschaftlichen Sicherheitsvorsorge fordert das Weißbuch eine resiliente Gesellschaft, zu deren Erreichen auch ein wirkungsvoller Zivil- und Katastrophenschutz gehören.“ **(Zitat: Dr. Wolfram Geier, Leiter der Abteilung II „Notfallvorsorge, Kritische Infrastrukturen“ im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. – BBK Bevölkerungsschutz 2/2014 * Editorial)**

Aufgrund des Ukraine-Kriegs und der zunehmenden Beteiligung durch NATO und Europäische Union ist die Gefahr einer Eskalation nicht zu unterschätzen. Sollten die Europäische Union sowie die Bundesregierung sich nicht verstärkt diplomatisch für Friedensverhandlungen einsetzen, so ist die Wahrscheinlichkeit hoch, als NATO-Partner in einen Krieg mit Russland hineingezogen zu werden. Der Einsatz von atomaren Waffen wäre folglich zu befürchten.

Aufgrund dieser Tatsache rückt die Versorgung der Bevölkerung nicht nur im Falle von Freisetzung radioaktiver Stoffe aus einem Kernkraftwerk in den Fokus, sondern wegen extremer Strahlenbelastung durch Einsatz von Nuklearwaffen auf dem Gebiet der Ukraine.

Des Weiteren sind auf deutschem Boden US-Atomwaffen stationiert. Hierdurch wird Deutschland ein potenzielles Angriffsziel russischer Fernlenkwaffen. Gleiches gilt für Frankreich.

Überblick über das Ergebnis der Risikoanalyse „Freisetzung radioaktiver Stoffe aus einem Kernkraftwerk, Szenario ‚Ländlicher Raum, Sommer'":

Schutzgut	Schadensparameter		Schadensausmaß A	B	C	D	E
MENSCH	M_1	Tote	■	■	■		
	M_2	Verletzte, Erkrankte	■	■	■	■	
	M_3	Hilfebedürftige	■	■	■	■	
	M_4	Vermisste	■				
UMWELT	U_1	Schädigung geschützter Gebiete	■	■	■		
	U_2	Schädigung von Oberflächengewässern/Grundwasser	■	■			
	U_3	Schädigung von Waldflächen	■	■	■		
	U_4	Schädigung landwirtschaftlicher Nutzfläche	■	■	■	■	■
	U_5	Schädigung von Nutztieren	■	■	■	■	■
VOLKS-WIRTSCHAFT	V_1	Auswirkungen auf die öffentliche Hand	■	■	■	■	
	V_2	Auswirkungen auf die private Wirtschaft	■	■	■	■	
	V_3	Auswirkungen auf die privaten Haushalte	■	■			
IMMATERIELL	I_1	Auswirkungen auf die öffentliche Sicherheit und Ordnung	■	■	■		
	I_2	Politische Auswirkungen	■	■	■	■	
	I_3	Psychosoziale Auswirkungen	■	■	■	■	■
	I_4	Schädigung von Kulturgut	■	■	■		

Quelle: Drucksache 18/7209 Deutscher Bundestag, 18. Wahlperiode

Überblick über das Ergebnis der Risikoanalyse „Freisetzung radioaktiver Stoffe aus einem Kernkraftwerk, Szenario ‚Urbaner Raum, Winter'":

Schutzgut	Schadensparameter		Schadensausmaß A	B	C	D	E
MENSCH	M_1	Tote	■	■	■		
	M_2	Verletzte, Erkrankte	■	■	■	■	
	M_3	Hilfebedürftige	■	■	■	■	■
	M_4	Vermisste	■				
UMWELT	U_1	Schädigung geschützter Gebiete	■	■	■		
	U_2	Schädigung von Oberflächengewässern/Grundwasser	■	■	■		
	U_3	Schädigung von Waldflächen	■	■	■		
	U_4	Schädigung landwirtschaftlicher Nutzfläche	■	■	■	■	■
	U_5	Schädigung von Nutztieren	■	■			
VOLKS-WIRTSCHAFT	V_1	Auswirkungen auf die öffentliche Hand	■	■	■	■	
	V_2	Auswirkungen auf die private Wirtschaft	■	■	■	■	
	V_3	Auswirkungen auf die privaten Haushalte	■	■	■		
IMMATERIELL	I_1	Auswirkungen auf die öffentliche Sicherheit und Ordnung	■	■	■		
	I_2	Politische Auswirkungen	■	■	■	■	
	I_3	Psychosoziale Auswirkungen	■	■	■	■	■
	I_4	Schädigung von Kulturgut	■	■	■		

Quelle: Drucksache 18/7209 Deutscher Bundestag, 18. Wahlperiode

„Die Kapazitäten der Notfallstationen, in denen die Dekontamination betroffener Einwohner und Einsatzkräfte sowie eine erste medizinische Betreuung betroffener Personen stattfindet (Screening von äußerlichen Kontaminationen und medizinische Beratung), werden angesichts der großen Zahl der zu behandelnden Personen schnell überschritten. Verfügbares medizinisches Personal wird in den Notfallstationen zusammengezogen, was zu Einschränkungen der medizinischen Versorgung in anderen Bereichen führt. Die Verfügbarkeit einer ausreichenden Zahl medizinischen Personals mit den erforderlichen strahlen-medizinischen Kenntnissen ist nicht sichergestellt. (…)

Ernährung:
Auch über das vorläufige und langfristige Sperrgebiet hinaus hat das Ereignis, vor allem im Szenario „Ländlicher Raum, Sommer“(,) massive und nachhaltige Auswirkungen auf die landwirtschaftliche Erzeugung in großen Teilen Deutschlands sowie den nördlich, östlich und westlich gelegenen Nachbarstaaten. Im Szenario „Ländlicher Raum, Sommer“ sind ca. 60 %, im Szenario „Urbaner Raum, Winter“ ca. ein Drittel der landwirtschaftlich genutzten Fläche in Deutschland in unterschiedlicher Intensität kontaminiert. Die Versorgung der Bevölkerung in Deutschland mit Grundnahrungsmitteln (Milch, Fleisch, Getreide) kann, insbesondere im Szenario „Ländlicher Raum, Sommer“ nicht in gewohntem Umfang erfolgen. Zur Sicherung der Versorgung werden zusätzliche Importe erforderlich. Die Absatzmöglichkeiten für legal vermarktungsfähige, aber belastete Lebensmittel sind eingeschränkt bzw. nicht gegeben. Die Verbraucher werden bevorzugt auf nachweislich nicht belastete Lebensmittel, die aus nicht vom Unfall betroffenen Regionen stammen, zurückgreifen, soweit sie sich diese höherpreisigen Produkte leisten können. Finanzielle Ausgleichsmaßnahmen werden insbesondere für die betroffenen landwirtschaftlichen Betriebe erforderlich. Im Szenario „Ländlicher Raum, Sommer“ hat das Ereignis schwerwiegende Folgen für die Land- und Ernährungswirtschaft in Deutschland und deren Position auf dem internationalen Markt.

Gesundheit:
Das Gesundheitssystem ist infolge des Ereignisses kurz-, mittel- und langfristig durch die medizinische und psychosoziale Versorgung sehr vieler Menschen stark gefordert und belastet. Dies gilt insbesondere in Bezug auf die Überwachung der Gesundheit der Bevölkerung sowie für die psychosoziale Unterstützung von Menschen, die z. B. durch den Verlust des Wohnortes oder durch Ängste belastet sind. In der Bevölkerung ist insbesondere im Bereich psychischer Belastung langfristig mit negativen Folgen zu rechnen, die nicht direkt durch die Strahlenexposition ausgelöst werden, sondern aufgrund der massiven Störung der sozialen und gesellschaftlichen Strukturen durch den Unfall und der Auswirkungen auf die eigene Existenz. Diese sind numerisch gravierender als die radiologisch bedingten gesundheitlichen Auswirkungen. In der Versorgung mit Arzneimitteln und Medizinprodukten sowie mit persönlichen Schutzausrüstungen für Einsatzkräfte entstehen aufgrund der hohen Nachfrage Engpässe.

Entsorgung kontaminierter Abfälle/Dekontamination von Flächen und Gebäuden:
Insbesondere in den hauptbetroffenen Gebieten, aber auch in Gebieten die weit darüber hinausgehen (Gebiete in mehreren Bundesländern), sind für die hier betrachteten Szenarien massive Aufräum- und Dekontaminationsarbeiten, auch zum Schutz der Bevölkerung und ihrer Lebensgrundlagen, erforderlich. Die Lagerung und Beseitigung der extrem großen Mengen (in der Größenordnung von mehr als 10 Millionen Kubikmetern, wie das Beispiel Fukushima zeigt) vor allem niedrig kontaminierter Abfälle (Böden, Pflanzen, Bodenbeläge etc.) ist eine sehr große Herausforderung. Gleiches gilt für die Bereitstellung entsprechend großer personeller Ressourcen zur Beseitigung kontaminierter Abfälle.“[37]

[37] „Bericht zur Risikoanalyse im Bevölkerungsschutz 2015“ (Drucksache 18/7209 des Bundestags, 04.01.2016, https://dserver.bundestag.de/btd/18/072/1807209.pdf)

Weiterführende Informationen (Literaturverzeichnis) zu dem gesamten Thema KRITIS finden Sie auszugsweise hier:

- Ausschuss für Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz, und Zivile Verteidigung (AFKzV) (2014): 34. Sitzung 19./20.03.2014, Beschluss zu TOP 7: Rahmenkonzeption für den CBRN-Schutz im Zivilschutz.
- Amtsblatt der Europäischen Union L197/1 vom 04.07.2012: Richtlinie 2012/18/EU des Europäischen Parlaments und des Rates zur Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen, zur Änderung und anschließenden Aufhebung der Richtlinie 96/82/EG des Rates.
- Amtsblatt der Europäischen Union L 293/1 vom 22.10.2013: Beschluss Nr. 1082/2013/EU des Europäischen Parlaments und des Rates. Amtsblatt der Europäischen Union L 347/924 vom 20.12.2013: Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17.12.2013 über ein Katastrophenschutzverfahren der Union.
- Amtsblatt der Europäischen Union L13/1: Richtlinie 2013/59/Euratom des Rates vom 5.12.2013 zur Festlegung grundlegender Sicherheitsnormen für den Schutz vor den Gefahren einer Exposition gegenüber ionisierender Strahlung und zur Aufhebung der Richtlinien 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom und 2003/122/Euratom.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.) (2011): BBK-Glossar: Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. Bonn.
- Bundesamt für Strahlenschutz (BfS) (Hrsg.): Aktualisierung der Quelltermbibliothek des Entscheidungshilfesystems RODOS für Ereignisse im Leistungsbetrieb – Vorhaben 3609S0009. Köln 2010. Bundes-Immissionsschutzgesetz (BImSchG) (1974), zuletzt geändert durch Art. 76 V. v. 31.08.2015 (BGBI) I S. 1474.
- Center for Security Studies (CSS) der ETH Zürich, Crisis and Risk Network (CRN) (2009): CRN Report – Focal Report 2: Risk Analysis – Integrated Risk Management and Societal Security.
- Zürich, S. 6 Council of the European Union: Draft Council conclusions on risk management capability – Adoption, Brussels, 26.09.2014 (OR. en) 13375/14 COR 1 PROCIV 77 JAI 688.
- Deutscher Bundestag: Plenarprotokoll 17/162, S. 19293 Erhardt, H.-G. und G. Neuneck (Hrsg.): Analyse sicherheitspolitischer Bedrohungen und Risiken unter Aspekten der Zivilen Verteidigung und des Zivilschutzes, Baden-Baden, 2015.
- Kaplan, D. E.: Aum Shinrikyo 1995 (2002). In: Tucker, J. B. (Hrsg.): Toxic terror: assessing terrorist use of chemical and biological weapons. Cambridge, S. 207 ff.
- M. Müller et. (2015): Arzneimittel-Lieferengpässe - Katastrophe für den Katastrophenschutz? In: Notarzt 31 (02), S. 66-68.
- Okumura et al. (1996): Report on 640 victims of the Tokyo subway sarin Attack. In: Ann Emerg Med 28 (2), S 129-135.
- Sicherheitsüberprüfungsfeststellungsverordnung (SFÜV) (2003), neugefasst durch V. v. 12.09.2007 I 2294, zuletzt geändert durch Art. 1 G v. 03.12.2015 I 2186 Sicherheitsüberprüfungsgesetz (SÜG) (1994), zuletzt geändert durch Art. 2 G v. 03.12.2015 I 2161.
- Störfall-Kommission (SFK) (1995): Leitfaden Anlagensicherheit, SFK – GS - 06, verabschiedet auf der 16. Sitzung der Störfall-Kommission am 12.09.1995. (http://www.kas-bmu.de/publikationen/sfk/sfk_gs_06.pdf, zuletzt abgerufen am 30.11.2022).
- Störfall-Kommission (SFK) (2002):Leitfaden - Maßnahmen gegen Eingriffe Unbefugter, SFK – GS - 38, verabschiedet auf der 41. Sitzung der Störfall-Kommission am 23.10.2002. (http://www.kas-mu.de/publikationen/sfk/sfk_gs_38.pdf, zuletzt abgerufen am 30.11.2015).
- Deutscher Bundestag (2014): Drucksache 18/3682.