Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

STELLUNGNAHME

**vom 6. Februar 2023 zu**

# Eckpunktepapier des zukünftigen KRITIS-Dachgesetzes

DVGW Deutscher Verein des
Gas- und Wasserfaches e.V.

**Ansprechpartner**
**Johanna Kreienborg (Wasser)**
**Hiltrud Schülken (Gas)**
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-900

E-Mail: johanna.kreienborg@dvgw.de; hiltrud.schuelken@dvgw.de

**Einleitung**
Der DVGW begrüßt grundsätzlich die Impulse des BMI-Eckpunktepapiers vom 07.12.2022 zum KRITIS-Dachgesetz für den physischen Schutz kritischer Infrastrukturen.

Das zukünftige KRITIS-Dachgesetz soll als Umsetzung der CER-Richtlinie dabei aber nicht nur den physischen Schutz kritischer Infrastrukturen regeln, sondern im Zusammenhang mit dem Fünf-Punkte-Plan der Europäischen Kommission[1] auch einer neuen Bedrohungsintensität begegnen, die sich aus einem hochprofessionellen Täterprofil und der Bedrohung von zivilen Infrastrukturen durch hybride Bedrohungen ergibt. Physische Bedrohungen und Cyberbedrohungen sind zunächst den sogenannten hybriden Bedrohungen zuzuordnen, wenn sie direkt oder indirekt (z.B. durch irreguläre Stellvertreter) durch fremde Staaten gesteuert werden. Auch wenn diese in Intensität und Qualität die völkerrechtliche Definition von kriegerischen Handlungen unterlaufen, können sie in der Summe erheblichen politischen, gesellschaftlichen oder wirtschaftlichen Schaden erzeugen. Um die Wirkung zu maximieren und gleichzeitig das Risiko zu minimieren, den Schwellenwert von kriegerischen Handlungen zu überschreiten, werden bei hybriden Bedrohungen verschiedene Handlungsräume verschaltet und miteinander verschnitten (etwa Cyberraum, physischer Raum oder Informationsraum).

Vor diesem Hintergrund bedarf es eines konvergenten und ganzheitlichen Ansatzes für das Meldewesen, die Lagebeurteilung und die Eindämmung, der alle für den sicheren Betrieb von kritischen Infrastrukturen einschlägigen Handlungsräume umfassend berücksichtigt. Zusätzlich sollte die Notstandsgesetzgebung der 1960er Jahre vor dem Hintergrund hybrider Bedrohungen auf den Stand des 21. Jahrhunderts gehoben werden. Insbesondere im Zusammenhang mit der Beurteilung der Systemsicherheit müssen die zuständigen Behörden auch die komplexen sowie reziproken cyber-physischen Wechselwirkungen bei der Netz- und Erzeugungsinfrastruktur beurteilen können.

Es geht im KRITIS-Dachgesetz um mehr verbindlichen Schutz für kritische Infrastrukturen und damit u.a. um die Sektoren Energie und Trinkwasser. Mit einem integrierten, ganzheitlichen Sicherheitsansatz sollten die sektorübergreifenden Abhängigkeiten Berücksichtigung finden und ein einheitlicher Mindeststandard in den Sektoren gesetzt werden. Die Resilienz von kritischen Infrastrukturen, das Vorhalten von Redundanzen, die Diversifizierung von Lieferketten und die Zusammenarbeit zwischen staatlichen Stellen und Betreibern kritischer Infrastrukturen sind dabei als essenziell zu betrachten und sollten im KRITIS-Dachgesetz entsprechend gewürdigt werden.

**Position des DVGW**
Um diesen Ansprüchen gerecht werden zu können, sollte ein zukünftiges KRITIS-Dachgesetz aus Sicht des DVGW folgende Anforderungen erfüllen:

1. Technische Regelsetzung als wesentliches Instrument zur Umsetzung des KRITIS-Dachgesetzes
2. Harmonisierung der gesetzlichen Anforderungen an den physischen Schutz und Cybersicherheit für die effektive Umsetzbarkeit durch die Gas- und Wassersektoren
3. Rechtliche Verankerung und Absicherung für Investitionen in physischen Schutz
4. Geeignete Behördenzuständigkeit und die behördenübergreifende Zusammenarbeit für die einheitliche Umsetzung auf allen administrativen Ebenen
5. Sicherstellung der einheitlichen Umsetzung der zukünftigen Regelungen zum physischen Schutz kritischer Infrastrukturen auf allen administrativen Ebenen von Bund, Ländern und Kommunen
6. Vereinheitlichung des Melde- und Nachweiswesen und Integrierung in bestehende Prozesse, ein Vorfall, eine Meldung!
7. Staatliche Verantwortung für die Abwehr von Sabotageakten mit terroristischer, kriegerischer, und/oder staatlicher Dimension

[1] Kommission ruft Mitgliedstaaten zu besserem Schutz kritischer Infrastrukturen auf (europa.eu)

8. Kohärenz der Anforderungen an Risikobewertung, Resilienzpläne, Schutzstandards und spezifische Regelungen
9. Verhältnismäßigkeit bei Transparenzpflichten für KRITIS-Betreiber
10. Begriffliche Konkretisierung kritischer Komponenten und maßvolle Beschaffungsvorbehalte
11. Neuregelung der Gefahrenabwehr im Einklang mit europäischen und internationalen Strategien

**Zu den Punkten im Einzelnen**

**1. Technische Regelsetzung als wesentliches Instrument zur Umsetzung des KRITIS-Dachgesetzes**

Für KRITIS-Betreiber sind sowohl die Harmonisierung der Gesetzgebung zur Cybersicherheit und zum physischen Schutz als auch die Identifizierung geeigneter branchenspezifischer Anforderungen an die physische Sicherheit entscheidende Handlungsfelder eines KRITIS-Dachgesetzes.

Die Ausgestaltung im Detail sollte über die seit Jahrzehnten bewährte Technische Regelsetzung in der Gas- und Wasserversorgung erfolgen. Der Verweis auf allgemein anerkannte Regeln der Technik und die entsprechende Ausgestaltung und Schaffung von Standards durch die Technische Regelsetzung haben sich in der Abwasserentsorgung und Trinkwasserversorgung sowie in der Gas- und Stromversorgung bewährt. Dies sollte in dem KRITIS-Dachgesetz in einer Formulierung analog dem § 49 Energiewirtschaftsgesetz ermöglicht werden.

Die Technischen Regeln des DVGW machen heute schon weiterführende Vorgaben zur Resilienz der Infrastruktur (DVGW W 1050 oder DVGW W 1003) sowie zum Risiko- und Krisenmanagement in der Gas-, Wasserstoff- und Trinkwasserversorgung (DVGW G 1001, G 1002, G 1003, W 1001). Solche Technischen Regeln und deren Weiterentwicklung innerhalb der jeweiligen Branchen sollten daher ein wesentlicher Bestandteil für die Umsetzung des KRITIS-Dachgesetzes sein, um eine effektive Umsetzung der gesetzlichen Regelungen und eine Verbesserung der Sicherheitslage in der Praxis zu ermöglichen.

**2. Harmonisierung der Anforderungen an physischen Schutz und Cybersicherheit für die effektive Umsetzbarkeit durch die Gas- und Wassersektoren**

Eine Harmonisierung des KRITIS-Dachgesetzes mit anderen Rechtsakten ist entscheidend für eine effektive und wirtschaftliche Umsetzbarkeit. Dabei sollten insbesondere die NIS 2.0-Richtlinie, der Cyber Resilience Act, aber auch weitere spezialrechtliche Regelungen (z. B. Network Code on Cybersecurity, IT-Sicherheitskataloge gemäß §§ 11 Absatz 1a/1b EnWG oder Kritische Komponenten nach § 11 Abs.1g EnWG) unbedingt berücksichtigt werden.

Die Anforderungen an Betreiber kritischer Infrastrukturen und die Compliance-Nachweise sollten ausreichend mit den bestehenden Vorgaben aus der aktuellen Cybersicherheitsregelung harmonisiert werden, um eine Erfüllung der zusätzlichen und teilweise auch neuartigen Anforderungen durch die Betreiber kritischer Infrastrukturen vor dem Hintergrund begrenzter Ressourcen (u.a. personell bedingt durch Fachkräftemangel, oder auch von begrenzten wirtschaftlichen Spielräumen) zu ermöglichen.

Darüber hinaus sollte darauf geachtet werden, dass bereits bestehende Detail-Regelungen nicht erneut, ggf. sogar widersprüchlich geregelt werden (Vermeidung von Mehrfachregelungen). Deshalb ist es unabdingbar, Betreiber und Branchenverbände frühzeitig und umfassend in die Ausgestaltung der Anforderungen im KRITIS-Dachgesetz mit einzubeziehen. Dabei müssen die bisherigen und in den Verbänden vorliegenden Erfahrungen aus vorherigen Gesetzgebungsverfahren (z. B. Smart Meter Gateway, Systeme zur Angriffserkennung) berücksichtigt werden. Neue Anforderungen müssen die Möglichkeit bieten, in bestehende

Managementsysteme (z. B. gemäß IT-Sicherheitskataloge oder ISO/IEC 27001) integriert zu werden. Nur hierdurch kann eine verhältnismäßige Regelung sichergestellt werden.

### 3. Rechtliche Verankerung und Absicherung für die Investition in physischen Schutz

Das neue KRITIS-Dachgesetz sollte für die Betreiber kritischer Infrastrukturen sowohl im nicht regulierten als auch im regulierten Bereich die notwendige rechtliche Sicherheit und Unterstützung bzw. Kostenanerkennung für Investitionen in die Resilienzerhöhung der physischen Sicherheit und die Abwehr von Bedrohungen sowie für Abhilfemaßnahmen zur Aufrechterhaltung des Betriebes im Falle eines erfolgreichen Angriffes geben. Dabei sollten auch Kosten anerkannt werden, welche über betriebliche Mittel und Maßnahmen für den Normalbetrieb hinausgehen. Solche Maßnahmen verhelfen zu mehr Versorgungssicherheit, wie etwa bei hybriden Bedrohungen, Cyberangriffen oder terroristischen Anschlägen.

### 4. Geeignete Behördenzuständigkeit und behördenübergreifende Zusammenarbeit

Die Bundeszuständigkeit im zukünftigen KRITIS-Dachgesetz soll laut dem Eckpunktepapier beim BBK liegen, dass damit als übergeordnete KRITIS-Behörde im Sinne des zukünftigen Dachgesetzes erst noch aufgestellt werden soll.

Bei der Zuordnung der Zuständigkeit ist es wesentlich, dass die Aufsichtsbehörde mit der notwendigen Fachkompetenz, Personal und Finanzmitteln für die Erfüllung ihrer Aufgaben ausgestattet ist.

Hierbei sind auch sonstige Zuständigkeiten aus spezialrechtlichen Regelungen wie etwa des Energiewirtschaftsgesetzes und die entsprechenden Anforderungen an die technische Gestaltung von kritischer Infrastruktur zu berücksichtigen. Branchenspezifische Schutzmaßnahmen sind sinnvoll, solange keine widersprüchlichen Anforderungen gestellt werden und keine konkurrierenden Zuständigkeiten sowie Interessen entstehen.

### 5. Sicherstellung der einheitlichen Umsetzung der zukünftigen Regelungen zum physischen Schutz kritischer Infrastrukturen auf allen administrativen Ebenen von Bund, Ländern und Kommunen

Die Erfahrung aus der Corona-Pandemie hat gezeigt, dass die Abstimmung zwischen den administrativen Ebenen (Bund, Ländern, Landkreisen sowie Kommunen) oftmals von großen Reibungsverlusten, unterschiedlichen Auslegungen und Umsetzungen der Vorschriften gekennzeichnet war. Ein konkretes Beispiel hierfür war die unterschiedliche Ausstellungspraxis von KRITIS-Bescheinigungen durch die Landkreisämter bzw. Ministerien. In vielen Fällen war auch unklar, wer diese KRITIS-Bescheinigungen ausstellt. Ein zukünftiges KRITIS-Dachgesetz sollte aus dieser Erfahrung Lehren ziehen, um klare und einheitliche Regelungen, Zuständigkeiten sowie Umsetzungen zu schaffen.

### 6. Vereinheitlichung des Melde- und Nachweiswesen und Integrierung in bestehende Prozesse, ein Vorfall, eine Meldung!

Insbesondere vor dem Hintergrund der steigenden Bedeutung hybrider Bedrohungen, muss ein KRITIS-Dachgesetz die Zuständigkeiten für alle möglichen Bedrohungsräume (Informationsraum, physischer Raum und Cyberraum) in einer Behörde oder einer effektiven behördenübergreifenden Zusammenarbeit bündeln. Dies gilt insbesondere für das zukünftige Meldewesen.

Die Betreiber kritischer Infrastrukturen müssen insbesondere Sicherheitsvorfälle zentral an nur eine Stelle melden können. Nur so kann beim Staat ein einheitliches und ganzheitliches Lagebild entstehen. Das IT-Sicherheitsgesetz sieht z.B. vor, dass für die Meldung von IT-Sicherheitsvorfällen eine zentrale Meldestelle besteht[2], die dann unter der Berücksichtigung sektorspezifischer Merkmale von Vorfällen, Informationen an die zuständigen Fachbehörden auf

[2] In diesem Fall das BSI - Bundesamt für Sicherheit in der Informationstechnik.

Bundes- oder Landesebene weiterleitet. Dieses Vorgehen hat sich bisher bewährt und sollte in ähnlicher Weise in einem Ansatz fortgeschrieben werden, in dem physischer Schutz und Cyberschutz in einem ganzheitlichen Melde- und Lagebildwesen zusammengeführt werden. In diesem Zusammenhang ist auch die Einrichtung eines behördenübergreifenden nationalen Sicherheitslagezentrums in Erwägung zu ziehen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z. B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte.

**7. Staatliche Verantwortung für die Abwehr von Sabotageakten mit terroristischer, kriegerischer, und/oder staatlicher Dimension und hybriden Bedrohungen**

Das Eckpunktepapier betont die besondere Verantwortung des Staates. Dieser Verantwortung soll der Staat durch das Angebot von Analysen, Leitfäden, Beratung, Übungen und Schulungen für die Betreiber Kritischer Infrastrukturen nachkommen.

Die im Eckpunktepapier erwähnte und im Verantwortungsbereich der KRITIS-Sektoren liegende Umsetzung geeigneter und verhältnismäßiger Schutzmaßnahmen sollte sich nicht auf die Abwehr von Sabotageakten mit terroristischer, kriegerischer, und/oder staatlicher Dimension und/oder hybrider Bedrohungen beziehen. da dies die Betreiber kritischer Infrastrukturen nicht umsetzen können und zudem auch im Sinne geeigneter Abwehr- bzw. Abschreckungsmechanismen an bestehende rechtliche Grenzen stößt (z. B. Drohnenabwehr oder der Einsatz militärischer Abwehrsysteme). Hier hat der Staat eine besondere Verantwortung zur Unterstützung der Betreiber.

Ferner müssen Voraussetzungen geschaffen werden, damit die im Eckpunktepapier erwähnten Maßnahmen auch umgesetzt werden können. Dies betrifft insbesondere den für den Cyberschutz und physischen Schutz gleichermaßen wichtigen Aspekt der Sicherheitsüberprüfungen. Hier liegt es an den zuständigen Bundesbehörden, die notwendigen Ressourcen bereitzustellen.

**8. Kohärenz von Anforderungen an Risikobewertung, Resilienzplänen, Schutzstandards und spezifischen Regelungen**

KRITIS-Betreiber müssen ihre spezifischen Schutzmaßnahmen an den Risikobewertungen, die im Rahmen des betrieblichen Risikomanagements entwickelt werden und an den zu definierenden europaweit einheitlichen Mindestvorgaben (verpflichtende Schutzstandards) ausrichten. Die spezifischen Schutzmaßnahmen sollen dabei geeignet und angemessen sein.

Darüber hinaus wird im Eckpunktepapier die Erstellung von Resilienzplänen für die stetige Erhöhung der Resilienz gefordert. Offen bleibt jedoch, wer für die Erstellung dieser Resilienzpläne verantwortlich ist. Zudem bleibt unklar wie das Zusammenspiel dieser Resilienzpläne, mit den aus den Risikobewertungen resultierenden Risikobehandlungsplänen, dem stetig anzupassenden verpflichtenden europaweiten Schutzstandard und den zutreffenden weitergehenden sektorspezifischen Regelungen aussehen kann. Um den Betreibern kritischer Infrastrukturen Orientierung und Handlungssicherheit zu geben, sollte dieser Prozess detaillierter ausformuliert werden, wie z. B. über die Technische Regelsetzung (siehe auch Punkt 1.).

Ein zukünftiges KRITIS-Dachgesetz sollte die Themenbereiche der physischen Sicherheit und Cybersicherheit im Sinne eines ganzheitlichen und integrierten Sicherheitsansatzes aufeinander abstimmen, um eine effiziente Umsetzung bei den KRITIS-Betreibern zu ermöglichen. Das betrifft insbesondere die wechselseitige Anerkennung von einzelnen Nachweisen bei den unterschiedlichen Aufsichtsbehörden (im Energiesektor z. B.: BBK, BSI, BNetzA).

**9. Verhältnismäßigkeit bei Transparenzpflichten für KRITIS-Betreiber**

Wie Sabotageakte in jüngerer Vergangenheit gezeigt haben, stellt die Bereitstellung von sensiblen Daten, die Aufschluss über Sicherheitsmaßnahmen und kritische Prozesse kritischer Infrastrukturen geben, ein essenzielles Risiko für den zuverlässigen und sicheren Betrieb kritischer Infrastrukturen dar.

Gegenwärtig unterliegen Betreiber kritischer Infrastrukturen sowohl auf Ebene des Bundes als auch auf Ebene der Länder einer Vielzahl von Informationsfreiheits- und Transparenzgesetzen (auf Bundesebene z. B. das IFG, das GeoZG und das UIG). Darüber hinaus bestehen aber auch speziellere Normen, die eine Datenherausgabe anordnen. Dies schließt etwa Informationen zur Art, zur gegenwärtigen Nutzung, zur tatsächlichen Verfügbarkeit und zur geografischen Lage des Standortes und der Leitungswege dieser Einrichtungen ein.
Für kritische Infrastrukturen bestehen jedoch in einigen Fällen Ausnahmen, was die Herausgabe bestimmter sensibler Daten betrifft. Allerdings müssen teilweise auch in diesen Ausnahmefällen die Informationen erst an eine zentrale Informationsstelle gesendet werden, um dann eine Ausnahmeantrag stellen zu können, damit diese Informationen nicht veröffentlicht werden (vgl. §§ 79 Abs. 2 S. 1/Abs. 3 Nr. 3 TKG).

Insgesamt sollte sichergestellt werden, dass Informationen über die kritischen Infrastrukturen nicht zu einfach über die Informationsfreiheits- und Transparenzgesetze zugänglich sind. Im Rahmen des KRITIS-Dachgesetzes sollten KRITIS-Betreiber von den tiefgreifenden gesetzlichen Transparenzpflichten ggf. ohne Stellung eines Antrags ausgenommen werden. Informationen über kritische Infrastrukturen sollten zudem nicht wie im Fall des § 79 Abs. 3 Nr. 3 TKG an einem zentralen Punkt gesammelt und gespeichert werden, bevor über ihre Veröffentlichung konkret entschieden wird. Würde diese Praxis im Rahmen des KRITIS-Dachgesetzes angewendet, so würden dadurch an einem einzigen Punkt viele sensible Informationen zusammenlaufen und ein „single point of failure“ geschaffen. Wird diese zentrale Informationsstelle kompromittiert, besteht Zugriff auf eine Vielzahl von Informationen über kritische Infrastrukturen von einer Vielzahl von Betreibern.

In verschiedenen Situationen fragen Behörden (z. B. Bundesbehörden oder Landeskriminalämter) bei Branchenexperten Informationen ab; allerdings verhindern z. B. Geheimhaltungspflichten und Quellenschutz das Teilen und den Austausch notwendiger Informationen zwischen den unterschiedlichen Behörden, mit Nachrichtendiensten und/oder mit den Fachexperten.
Das KRITIS-Dachgesetz sollte die Grundlage für einen geeigneten effizienten Informationsaustausch zwischen den für KRITIS zuständigen Behörden, mit Nachrichtendiensten und auch den Betreibern kritischer Infrastrukturen schaffen. Es sollte zudem vorsehen, dass die Informationen aus den Branchen zeitnah, abstrakt und anonymisiert den Branchen als Rückinformation wieder zur Verfügung gestellt werden, um einen beidseitigen Nutzen zu schaffen. Es würde z. B. dabei helfen, Sicherheitslücken, die bei einem Betreiber von kritischen Infrastrukturen aufgefallen sind, auch bei anderen Betreibern proaktiv zu schließen.

## 10. Begriffliche Konkretisierung kritischer Komponenten und maßvolle Beschaffungsvorbehalte

Im zukünftigen KRITIS-Dachgesetz sollte konkretisiert werden, was unter den kritischen Komponenten, die keine IT-Komponenten im Sinne des BSIG sind, zu verstehen ist. Mit der im Eckpunktepapier gegebenen Definition, könnten auch Baumaterialien und Rohstoffe unter eine Bestimmung kritischer Komponenten im Sinne des zukünftigen KRITIS-Dachgesetz fallen. Eine Definition sollte bei der Bestimmung der Kritikalität nur auf die Erbringung der kritischen Dienstleistung durch die betrachtete Komponente abstellen.

Bei der Festlegung der Beschaffungsvorbehalte im KRITIS-Dachgesetz, sollten Aufwand und Folgeschäden für die Betreiber kritischer Infrastrukturen – anders als bisher im IT-Sicherheitsgesetz – verhältnismäßig sein (bez. Einholung möglicher Garantieerklärungen, aufwändige Administration, Untersagung von Komponenteneinsatz). Beschaffungsvorbehalte bei kritischen Komponenten, die keine IT-Komponenten im Sinne des BSIG sind, dürfen den Beschaffungsprozess nicht unverhältnismäßig erschweren.
Es besteht auch die Gefahr, dass die Festlegungen in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen eingreift und ggf. zu Marktverzerrungen wegen Ungleichbehandlung führen.

Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend mit den Betreibern bzw. Branchenverbänden festgelegt und kommuniziert werden. Die Beschaffung der Komponenten und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der

Sicherheit – im Gefahrenfall – muss jederzeit möglich sein. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss verhältnismäßig und unter Wahrung einer ausreichenden Übergangsfrist erfolgen (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr, die Sicherheit in kritischen Infrastrukturen zu schwächen. Die Beschaffbarkeit kritischer Komponenten ist essenziell für die Versorgungssicherheit – bei vorliegenden Versorgungsengpässen für kritische Komponenten, sollte eine Güterabwägung zwischen Konformität der Vorgaben für kritische Komponenten und der Versorgungssicherheit im Sinne der Beschaffung erfolgen.

## 11. Neuregelung der Gefahrenabwehr im Einklang mit europäischen und internationalen Strategien erforderlich

Obwohl das Eckpunktepapier betont, dass das Gesamtsystem beim physischen Schutz kritischer Infrastrukturen im Vordergrund stehen muss, erwähnt das Papier leider nicht die aus Sicht eines Bundesgesetzes wesentliche Herausforderung, dass die Gefahrenabwehr im Sinne dieser Gesamtsystemperspektive und der neuen Bedrohungsintensität nicht mehr durch die alleinige Zuständigkeit der Länder erfolgen kann, sondern in Zukunft unter Beteiligung von Bundesbehörden und vor dem Hintergrund des Fünf-Punkte-Plans der Europäischen Kommission sogar durch europäische oder militärische Organisationen wie der NATO erfolgen muss. Außerhalb von NIS 2.0- und CER-Richtlinie muss der zukünftige Schutz kritischer Infrastrukturen auch die sicherheitspolitischen Risiken von strategischen Partnerschaften und gesellschaftsrechtlichen Übernahmen kritischer Infrastrukturen durch Drittstaaten angemessen berücksichtigen.