



Ausschussdrucksache 21(4)102 E
vom 28. November 2025

Schriftliche Stellungnahme

von Mathias Böswetter, BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Berlin vom 28. November 2025

Öffentliche Anhörung

zu dem

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen

BT-Drucksache 21/2510

und

Antrag der Abgeordneten Dr. Konstantin von Notz, Jeanne Dillschneider, Dr. Irene Michalic, Rebecca Lenhard, Sara Nanni und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Deutschland resilient machen – Für einen ganzheitlichen Schutz unserer kritischen Infrastruktur

BT-Drucksache 21/2725

Berlin, 28. November 2025

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
www.bdeu.de

Stellungnahme

Zur Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 1. Dezember 2025 zum KRITIS-Dachgesetz (KRITIS-DachG)

Transparenz-Register-ID des BDEW: 20457441380-38

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten mehr als 2.000 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 95 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Der BDEW ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung sowie im europäischen Transparenzregister für die Interessenvertretung gegenüber den EU-Institutionen eingetragen. Bei der Interessenvertretung legt er neben dem anerkannten Verhaltenskodex nach § 5 Absatz 3 Satz 1 LobbyRG, dem Verhaltenskodex nach dem Register der Interessenvertreter (europa.eu) auch zusätzlich die BDEW-interne Compliance Richtlinie im Sinne einer professionellen und transparenten Tätigkeit zugrunde. Registereintrag national: R000888. Registereintrag europäisch: 20457441380-38

Inhalt

1	Vorbemerkung	3
2	Positionen des BDEW	4
2.1	Regelschwellenwert nach § 5 Abs. 2 Satz 2 KRITIS-DachG-E.....	4
2.2	Transparenzpflichten und Schutz sicherheitsrelevanter Informationen	5
2.3	Drohnenabwehr und Finanzierung neuer Detektions- und Schutzsysteme ..	6
3	Fazit und Empfehlungen	6

1 Vorbemerkung

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) und seine Landesorganisationen vertreten über 2.000 Unternehmen der Strom-, Gas-, Wärme- sowie Wasser- und Abwasserwirtschaft in Deutschland. Die Mitgliedsunternehmen sichern rund 90 % des Strom- und über 95 % des Netzbetriebs sowie etwa 80 % der Trinkwasserversorgung in Deutschland.

Resiliente kritische Infrastrukturen der Energie- und Wasserwirtschaft sind eine Grundvoraussetzung für das Funktionieren aller Lebensbereiche und für die wirtschaftliche Leistungsfähigkeit des Standorts Deutschland sowie die Wettbewerbsfähigkeit des Energiestandorts Deutschlands.

Der Gesetzentwurf zur Umsetzung der Richtlinie (EU) 2022/2557 (KRITIS-DachG) schafft erstmals einen sektorenübergreifenden Rechtsrahmen für den physischen Schutz kritischer Anlagen und ergänzt damit das bestehende IT-Sicherheitsrecht für die kritischen Infrastrukturen.

Dieses Ziel begrüßen wir ausdrücklich. Positiv hervorzuheben sind u. a. der Ansatz einer engen Verzahnung mit der NIS2-Umsetzung, die für die Energiewirtschaft aus unserer Sicht durch die weitreichenden Bereichsausnahmen im Energiewirtschaftsgesetz zielführend geregelt wird.

Auch viele Anliegen des Bundesrates – etwa der Stärkung eines umfassenden KRITIS-Schutzes über die Fachgesetzgebung, der Schutz sicherheitsrelevanter Informationen sowie die Forderung nach Transparenz beim Erfüllungsaufwand und einer gesicherten Refinanzierung – werden von der Energie- und Wasserwirtschaft ausdrücklich geteilt.

Insbesondere die wirtschaftliche Umsetzung der Maßnahmen ist entscheidend für eine nachhaltige Resilienzsteigerung bei den kritischen Infrastrukturen. Denn Resilienz ist eine gesamtgesellschaftliche Aufgabe: Wirtschaft und Gesellschaft sind hierfür auf eine wirtschaftliche Versorgung mit Energie und Wasser sowie eine gesicherte Abwasserentsorgung angewiesen.

Deshalb muss das KRITIS-DachG den KRITIS-Betreibern nach einem risikobasierten Ansatz auch die Wahlmöglichkeit zwischen Maßnahmen der physischen Sicherheit oder des betrieblichen Kontinuitätsmanagements (auch Business Continuity Management / BCM genannt) offenhalten. Denn allein die KRITIS-Betreiber können beurteilen, welche konkreten präventiven, baulichen oder organisatorischen Maßnahmen angemessen und wirtschaftlich umsetzbar sind.

Zur Steigerung der Resilienz als gesamtgesellschaftliche Aufgabe muss schließlich die Zusammenarbeit zwischen den Behörden untereinander und mit den KRITIS-Betreibern weiter ausgebaut werden. Dies gilt insbesondere für die Erstellung umfassender Lagebilder. Die KRITIS-Betreiber kommen schon heute im Rahmen ihrer gesetzlichen Verpflichtungen an die Informationssicherheit umfangreichen Meldepflichten zu Vorfällen nach. Für ein umfassendes Lagebewusstsein sollte der bidirektionale Informationsaustausch zwischen Behörden und KRITIS-Betreibern aber zukünftig weiter gestärkt und die dafür genutzte IT-Infrastruktur den IT-Sicherheitsanforderungen genügen, die die KRITIS-Betreiber selbst zu erfüllen haben.

2 Positionen des BDEW

2.1 Regelschwellenwert nach § 5 Abs. 2 Satz 2 KRITIS-DachG-E

Der Regierungsentwurf sieht in § 5 Abs. 2 Satz 2 KRITIS-DachG-E als Regelschwellenwert „grundsätzlich 500 000 von einer Anlage zu versorgende Einwohner“ vor.

Dieser Wert dient als Leitplanke für die spätere Festlegung sektoren-, branchen- oder anlagenspezifischer Schwellenwerte durch eine Rechtsverordnung. Die Begründung stellt ausdrücklich klar, dass davon abweichende – ggf. auch niedrigere – Schwellenwerte sowie die Benennung einzelner Anlagenkategorien als kritisch möglich sind, wenn dies aus Sicht der Risikobetrachtung erforderlich sein sollte.

Der Bundesrat fordert demgegenüber eine Absenkung dieses gesetzlichen Regelschwellenwertes auf 150.000 versorgte Personen, um eine flächendeckendere Erfassung von Betreibern zu erreichen.

Aus Sicht der Energie- und Wasserwirtschaft sprechen insbesondere drei Punkte gegen eine Absenkung im Gesetz:

- **Fehlende belastbare Folgenabschätzung:** Der Entwurf hält fest, dass der Erfüllungsaufwand für die Wirtschaft derzeit „in seiner Gesamtheit noch nicht geschätzt werden kann“ und erst im Zuge der konkretisierenden Rechtsverordnungen belastbar zu quantifizieren ist. Bereits ohne Schwellenwertsenkung ist damit von erheblichen Investitions- und Betriebskosten auszugehen. Nach bisherigem Stand sollen etwa 1.700 Unternehmen unter das KRITIS-Dachgesetz fallen; eine Absenkung auf 150.000 würde den Kreis der betroffenen Unternehmen und Anlagen – insbesondere kleinerer und mittlerer Versorger ohne KRITIS-Vorerfahrung – deutlich ausweiten. Es droht eine massive gesamtwirtschaftliche Mehrbelastung, die einer nachhaltigen Resilienzsteigerung im Wege stehen wird.
- **Notwendige Kohärenz mit NIS2-Umsetzung und IT-Sicherheitsrecht:** Die Regelungen des KRITIS-Dachgesetzes orientieren sich ausdrücklich an den bisherigen IT-Sicherheitsvorgaben und sollen mit NIS2UmsuCG und BSIG kohärent sein. Der Versorgungsgrad von 500.000 Personen ist aus diesem Rechtsrahmen abgeleitet und gerichtsbewährt. Würde allein im KRITIS-Dachgesetz der Regelschwellenwert auf 150.000 abgesenkt, entstünden zwei grundlegend unterschiedliche Betreiberkreise für physische Resilienz und IT-Sicherheit. Bereits heute kritisiert der BDEW doppelte Begriffsbestimmungen und unklare Querverweise zwischen KRITIS-Dachgesetz, NIS2UmsuCG und weiteren Gesetzen. Eine einseitige Absenkung im KRITIS-Dachgesetz würde diesen Befund verschärfen und mittelbar Druck erzeugen, auch die NIS2-Schwellenwerte nach unten anzupassen – mit weiteren erheblichen Zusatzbelastungen.

- **Umsetzbarkeit und Fristen:** Die Betreiber kritischer Anlagen erhalten für die Umsetzung der Resilienzplichten nach Registrierung voraussichtlich lediglich rund zehn Monate Zeit. Dieses ambitionierte Zeitfenster ist schon für Unternehmen mit langjähriger KRITIS-Erfahrung herausfordernd. Eine gleichzeitige, abrupte Einbeziehung vieler neuer Betreiber ohne entsprechende Vorarbeit – oftmals zusätzlich belastet durch NIS2-, DORA- und weitere Vorgaben – würde die praktische Umsetzung erheblich gefährden.

Der BDEW plädiert daher dafür, den Regelschwellenwert von 500.000 versorgten Einwohnern im Gesetz beizubehalten und den legitimen Wunsch nach flächendeckender Versorgungssicherheit über die Verordnung nach § 5 KRITIS-DachG-E zu adressieren: Dort können – auf Basis der nationalen Risikoanalyse und sektorspezifischer Expertise der Branchenverbände – für bestimmte Sektoren oder Anlagentypen gezielt niedrigere Schwellenwerte oder einzelne Anlagenkategorien unabhängig vom Versorgungsgrad bestimmt werden.

2.2 Transparenzpflichten und Schutz sicherheitsrelevanter Informationen

Der Bundesrat weist zu Recht darauf hin, dass der Schutz sicherheitsrelevanter Informationen integraler Bestandteil eines wirksamen KRITIS-Schutzes sein muss. Angesichts der Möglichkeiten KI-basierter Suchmaschinen und Algorithmen, Informationen aus frei zugänglichen Quellen systematisch zu sammeln, aufzubereiten und für Angriffe zu nutzen – etwa zur Identifikation von Zielen oder zur Programmierung von Drohnen – gewinnen Transparenzpflichten eine neue sicherheitspolitische Qualität.

Aus Sicht der Energie- und Wasserwirtschaft ist eine umfassende und praxistaugliche Neubewertung bestehender Transparenzpflichten erforderlich. Transparenz-, Informationsfreiheits- und Open-Data-Regelungen sollten dort eingeschränkt oder angepasst werden, wo sie die physische oder IT-Sicherheit kritischer Infrastrukturen gefährden können. Webangebote von Behörden oder Open-Source-Plattformen, die systematisch Leistungsdaten oder Geolokationen kritischer Anlagen bereitstellen, müssen auf ein abstrahiertes und aus Sicherheitssicht vertretbares Maß reduziert werden.

Bei Portalen von Bundes- und Landesbehörden sollte grundsätzlich nachvollziehbar sein, wer Infrastrukturdaten abrufen kann.

Ausschreibungen und Konsultationen, die sensible Informationen zur Planung oder Umsetzung von Vorhaben der Kritischen Infrastruktur enthalten, sollten nur noch einem klar abgegrenzten Kreis von unmittelbar betroffenen KRITIS-Betreibern und Stakeholdern mit nachgewiesenem Interesse zugänglich gemacht werden.

Soweit die Bereitstellung von Informationen durch Betreiber kritischer Infrastrukturen die öffentliche Sicherheit oder Ordnung oder die Netz- und Informationssicherheit gefährden oder dem Wohl des Bundes oder eines Landes Nachteile bereiten würde, sollte keine Pflicht zur Informationsbereitstellung nach Informationsfreiheitsgesetzen bestehen. Die Risiken aus Transparenzpflichten – insbesondere im Zusammenspiel mit KI-gestützter Auswertung – sollten zudem ausdrücklich Gegenstand der Nationalen Risikoanalysen und der Resilienzstrategie gemäß CER-Richtlinie sein.

2.3 Drohnenabwehr und Finanzierung neuer Detektions- und Schutzsysteme

Die Bedrohung kritischer Anlagen durch unbemannte Luftfahrtsysteme hat vor dem Hintergrund der aktuellen sicherheitspolitischen Lage deutlich zugenommen. Der Bundesrat greift dies auf und bittet zu prüfen, inwieweit Betreiber kritischer Anlagen oder von ihnen eingesetzte, staatlich zertifizierte Sicherheitsdienste rechtssicher ermächtigt werden können, auffällige oder sicherheitsrelevante Drohnen zu detektieren, zu melden und technische Abwehrmaßnahmen einzuleiten. Zugleich unterliegt der Luftraum der Luftaufsicht des Bundes, sodass Maßnahmen der Drohnenabwehr durch Private nach aktueller Rechtslage regelmäßig rechtswidrig wären.

Der BDEW unterstützt das Anliegen einer zügigen gesetzlichen Klärung der Zuständigkeiten bei der hoheitlichen Aufgabe Drohnenabwehr, die für eine effektive Detektion und Abwehr von Drohnen bei den kritischen Infrastrukturen in der Fläche geeignet sind. Dabei ist aus unserer Sicht zentral, dass sich aus der Klärung keine generelle gesetzliche Verpflichtung zur Beschaffung und zum Betrieb von Drohnenabwehrsystemen für KRITIS-Betreiber ergibt. Betreiber müssen im Rahmen ihrer Risikoanalysen eigenständig entscheiden können, welche präventiven, baulichen, organisatorischen oder BCM-Maßnahmen angemessen und verhältnismäßig sind.

Für eine wirksame Resilienz der Energie- und Wasserwirtschaft ist dabei sicherzustellen, dass Investitionen in neue Detektions- und Schutzsysteme – einschließlich Systeme zur Drohnerkennung und -abwehr – als betriebsnotwendige Aufwendungen anerkannt und über regulierte Entgelte bzw. Gebühren und Entgelte in der Wasserwirtschaft refinanzierbar sind. Entsprechende Klarstellungen im Regulierungsrahmen des Energierechts sowie bei den entsprechenden Regelungen für die Wasserwirtschaft sind erforderlich. Angesichts der hybriden Bedrohungslage sollten solche Investitionen zudem als Beiträge zur Gesamtverteidigung verstanden und auch aus dem Verteidigungshaushalt kofinanziert werden.

3 Fazit und Empfehlungen

Vor dem Hintergrund der dargelegten Erwägungen empfiehlt der BDEW für das weitere Gesetzgebungsverfahren:

1. Beibehaltung des Regelschwellenwertes von 500.000 versorgten Einwohnern in § 5 Abs. 2 Satz 2 KRITIS-DachG-E und Ablehnung der vorgeschlagenen Absenkung auf 150.000 im Gesetzestext. Eine Erweiterung des Anwendungsbereichs sollte zielgenau über die Verordnung nach § 5 KRITIS-DachG-E erfolgen.
2. Transparente Quantifizierung des Erfüllungsaufwands für Wirtschaft und Verwaltung sowie Begrenzung der kumulativen Belastungen aus KRITIS-Dachgesetz, NIS2UmsuCG und weiteren Regelwerken auf das notwendige Maß.

3. Umfassende und praxistaugliche Neubewertung der Transparenzpflichten mit klaren Ausnahmen für sicherheitsrelevante Informationen zu kritischen Anlagen, einschließlich einer Anpassung einschlägiger Informationsfreiheits- und Open-Data-Regelungen.
4. Gesetzliche Klärung der Zuständigkeiten und Befugnisse für eine effektive Drohnenabwehr bei kritischen Infrastrukturen in der Fläche.
5. Sicherstellung der Refinanzierbarkeit und öffentlicher Mitfinanzierung von Resilienzinvestitionen, insbesondere für neue Detektions- und Schutzsysteme – etwa Drohnendetektion und -abwehr – durch Anerkennung als regulierungsfähige Kosten und Einbindung in nationale und bündnisbezogene Resilienz- und Verteidigungsbudgets.