Berlin, 4. September 2025

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

Gesetz des Bundesministeriums des Innern zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz)

Schreiben des BMI vom 29. August 2025
Verbändebeteiligung – KM4.51005/13#1

Transparenz-Register-ID des BDEW: 20457441380-38

Inhalt

1 Vorbemerkung 3

2 Positionen des BDEW 4

2.1 Abgrenzung kritische Anlage von Betriebsstätte 4

2.2 Prüfung der Querverweise zum NIS2-UmsuCG und anderen Gesetzen 4

2.4 Finanzierung und Kostenanerkennung neuer Detektions- und Schutzsysteme 5

2.3 Umfassende und praxistaugliche Neubewertung von Transparenzpflichten 6

2.4 Möglichkeit der Strafverfolgung gemäß Strafgesetzbuch 7

2.5 Fehlende Umsetzung im Gesetzestext der Zweiwegekommunikation . 7

2.6 Ganzheitliche und praxistaugliche Weiterentwicklung des Rechtsrahmens für personelle Sicherheit 7

2.7 Klärung der Zuständigkeiten bei der Drohnenabwehr und Möglichkeit zur Beleihung der Betreiber 8

2.8 Konfligierende Gesetzgebung zwischen Umwelt-, Straf- und KRITIS-Recht 9

2.9 Abgrenzung der Anforderungen von Behörden und KRITIS-Betreibern im Rahmen der Nationalen Risikoanalysen 9

2.10 Verbundunternehmen und technische Betriebsführer werden durch verschiedene Anforderungsregime auf Bundes- und Landesebene überfordert 10

2.11 Behördliche Abstimmung bzgl. maritimen Infrastrukturen 10

1 Vorbemerkung

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) begrüßt, dass das KRITIS-Dachgesetz nun endlich in die Verbändeanhörung gegeben wurde. Dieser Schritt hätte jedoch deutlich früher erfolgen müssen – zumal gegenüber dem Regierungsentwurf aus dem vergangenen Jahr nur marginale Änderungen erkennbar sind. Angesichts der aktuellen Bedrohungslage benötigen KRITIS-Betreiber schnellstmöglich Rechts- und Investitionssicherheit, damit der Schutz kritischer Infrastrukturen weiterhin vorausschauend gewährleistet werden kann. Aufgrund dieser Verzögerung und des Umstandes, dass die Umsetzungsfristen aus der CER-Richtlinie davon unberührt bleiben, entsteht den Betreibern kritischer Infrastrukturen eine Umsetzungsfrist der Resilienzpflichten von voraussichtlich lediglich 10 Monaten nach Registrierung.

Der BDEW bedauert zudem die sehr kurze Frist zur Stellungnahme. Der letzte Referentenentwurf, der den Verbänden im Dezember 2023 offiziell zugegangen ist, weicht erheblich vom Regierungsentwurf aus dem letzten Jahr ab, bei dem den Verbänden keine Möglichkeit zur Stellungnahme gegeben wurde.

Positiv hervorzuheben ist allerdings, dass die IT-Sicherheitskataloge der Bundesnetzagentur auch für die neuen Anforderungen an physische Sicherheit und Resilienz anerkannt werden sollen. Damit wird eine zentrale Position des BDEW aufgegriffen: Durch diese Anerkennung wird auf einem bewährten Fundament eine zügige, wirtschaftliche und bürokratiearme Umsetzung im Rahmen eines einheitlichen Nachweisverfahrens für Resilienz- und Cybersicherheitsanforderungen gegenüber der Bundesnetzagentur im Sektor Energie ermöglicht – und damit auch eine enge Verzahnung von KRITIS-Dachgesetz und NIS2-Richtlinien-Umsetzung.

Auch aus wasserwirtschaftlicher Sicht ist der Ansatz einer weitestmöglichen Anerkennung bestehender Branchenstandards und etablierter Frameworks zum Schutz kritischer Infrastrukturen sehr zu begrüßen.

Ebenso positiv hervorzuheben ist vor dem Hintergrund der aktuellen Bedrohungslage in Ost- und Nordsee die Berücksichtigung der maritimen Infrastrukturen. Für die Stärkung der Resilienz dieser essenziellen Infrastrukturen sind die Betreiber aber auch auf eine gute und enge Abstimmung zwischen der Bundesnetzagentur, dem Bundesamt für Seeschifffahrt und Hydrographie (BSH) sowie die Behörden im Maritimen Sicherheitszentrum (MSZ) angewiesen. In Bezug auf die maritime Sondersituation sollte im MSZ eine Koordinierungsstelle geschaffen werden, die, wie im Gesetz vorgesehen, eine behördeninterne Koordinierungsfunktion zu KRITIS-Fragen in der ausschließlichen Wirtschaftszone wahrnimmt.

Es ist schließlich grundsätzlich ein richtiges Signal, Investitionen in die Sicherheit kritischer Infrastrukturen nicht mehr bloß als Opportunitätskosten darzustellen. Allerdings hat die Kostenabschätzung des Erfüllungsaufwandes der Wirtschaft - die noch Bestandteil der vergangenen Entwürfe des KRITIS-Dachgesetzes war, in diesem zur Konsultation gegebenen Referentenentwurf aber bedauerlicherweise nicht mehr enthalten ist - auch gezeigt, dass die anstehenden Investitionen die deutsche Energiewirtschaft in einen deutlichen Wettbewerbsnachteil zu anderen Mitgliedsstaaten setzen könnten.

2 Positionen des BDEW

2.1 Abgrenzung kritische Anlage von Betriebsstätte

Sofern der Begriff der kritischen Anlage auf die konkrete Betriebsstätte verjüngt und nicht auf den weiteren infrastrukturellen Zusammenhang erweitert wird, droht eine regelmäßige Unterlaufung kritischer Anlagen des Versorgungsgrades von 500.000 Personen. Das bedeutet, dass praktisch keine kritische Anlage unter den Anwendungsbereich des Gesetzes fallen würde. Daher ist eine Ausweitung des Begriffs der kritischen Anlage auf den weiteren Begriff der versorgungsrelevanten Zusammenhänge der kritischen Infrastrukturen vorzunehmen.

2.2 Prüfung der Querverweise zum NIS2-UmsuCG und anderen Gesetzen

Eine redaktionelle Prüfung der jeweiligen Querverweise zwischen KRITIS-Dachgesetz und NIS2UmsuCG bezüglich Aktualität und Richtigkeit sollte erfolgen. Zudem ist keine hinreichende Abstimmung mit dem NIS2UmsuCG bzw. der BSI-Kritisverordnung erfolgt. Noch immer werden Begriffe doppelt definiert (z.B. „Betreiber einer kritischen Anlage“) und teilweise gleiche Paragrafen mit unterschiedlichem Inhalt eingeführt. So enthält sowohl das Gesetz zur Stärkung der Resilienz kritischer Anlagen als auch das NIS2-Umsetzungsgesetz einen § 5d EnWG mit jeweils unterschiedlichem Inhalt.

In diesem Sinne müsste auch eine Umformulierung §18 des KRITIS-Dachgesetzes erfolgen:

„Der Betreiber kritischer Anlagen ist verpflichtet, Vorfälle unverzüglich, spätestens 24 Stunden nach Kenntnis **der vom Bundesamt für Sicherheit der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichteten gemeinsamen Meldestelle nach § 32 Absatz 1 des BSI-Gesetzes** [in der Fassung des NIS2UmsuCG] zu melden.“

Ferner wurden auch die sonstigen Fachgesetze nicht angepasst. In verschiedensten gesetzlichen Regelungen wird der Begriff der kritischen Infrastruktur verwendet. Beispielhaft genannt seien §§ 17, 18 Zivilschutz- und Katastrophenhilfegesetz, § 55a Außenwirtschaftsverordnung, § 79 Abs. 3 TKG. Eine Anpassung dieser Begrifflichkeiten wird hier nicht vorgenommen und es verbleibt unklar, ob zukünftig der Begriff der kritischen Anlage aus der NIS2-Umsetzung oder dem KRITIS-Dachgesetz maßgeblich sein soll. Gleiches gilt für Landesgesetze.

Überdies widerspricht sich der Gesetzestext mit der beigefügten Begründung. Während es an einer Stelle heißt, dass „Maßnahmen verhältnismäßig sein …“ sollen, wird an anderer Stelle darauf verwiesen, „dass der Stand der Technik eingehalten werden …“ soll. Hier bedarf es einer zwingenden Klarstellung.

2.4 Finanzierung und Kostenanerkennung neuer Detektions- und Schutzsysteme

Für eine wirksame Resilienz der Energie- und Wasserwirtschaft sowie eine fortgesetzte Wettbewerbsfähigkeit des Energiestandorts Deutschlands in Europa ist zunächst sicherzustellen, dass Investitionen in neue Detektions- und Schutzsysteme oder personelle Prozesse als betriebsnotwendige Aufwendungen anerkannt und damit über die Entgelte refinanzierbar sind. Dies erfordert eine eindeutige Regelung zur Kostenanerkennung durch die Bundesnetzagentur und die Aufnahme solcher Maßnahmen in die Gebührenfähigkeit nach energiewirtschaftlichen und wasserrechtlichen Vorgaben. Dabei könnten Energienetzbetreiber der Bundesnetzagentur die sich aus den neuen Resilienzbedarfen ergebenden Netzinfrastrukturmerkmale zeitnah mitteilen.

Nur so können Betreiber kritischer Infrastrukturen mit Planungssicherheit investieren und gleichzeitig sicherstellen, dass die Refinanzierung im Rahmen der regulierten Entgeltsysteme gewährleistet ist.

Darüber hinaus muss die Finanzierung neuer Systeme, baulicher sowie personeller Maßnahmen und Prozesse durch den Staat flankiert werden. Angesichts der zunehmenden hybriden Bedrohungslage ist es erforderlich, dass solche Investitionen auch aus dem Verteidigungshaushalt gestützt werden. Hierbei ist der strategische Kontext der NATO maßgeblich: Mit der Beschlusslage zur 5 Prozent-Verteidigungsverpflichtung bis 2035, von der bis zu 1,5 Prozent des BIP für Resilienzmaßnahmen vorgesehen sind, eröffnen sich neue Finanzierungsräume. Neue Detektions- und Schutzsysteme wie Systeme zur Drohnendetektion und -abwehr für kritische Infrastrukturen fallen aus Sicht des BDEW unmittelbar in diesen Resilienztatbestand. Ihre Förderung ist daher sowohl national wie auch europäisch und transatlantisch als Bestandteil der

Gesamtverteidigung zu verankern und so als Beitrag zur Erreichung beschlossenen Ziele zur Stärkung des Verteidigungsbündnisses zu verstehen.

Die Infrastrukturen der Energie- und Wasserversorgung sind nicht nur für die Bevölkerung unverzichtbar, sondern auch für die Operationsfähigkeit der Bundeswehr und ihrer Verbündeten im Rahmen des Host Nation Supports / OPLAN Deutschland sowie für die Funktionsfähigkeit der Sicherheits- und Verteidigungsindustrie. Entsprechend muss die Kostenanerkennung durch die Bundesnetzagentur Hand in Hand mit der staatlichen Mitfinanzierung erfolgen, um sowohl die betriebliche Tragfähigkeit als auch die nationale und bündnisstrategische Resilienz sicherzustellen.

Für Deutschland bedeutet dies: Die energie- und wasserspezifische Resilienz ließe sich künftig national wie bündnisstrategisch finanzieren. Neue Schutzsysteme wie Systeme zur Detektion von Drohnen sollten als legitime Resilienzinvestitionen gelten, für die entsprechende Förderkulissen im Verteidigungshaushalt geschaffen werden müssen – im Sinne einer wirksamen Gesamtverteidigung, die zivile Infrastrukturen schützt und damit auch die Verteidigungsfähigkeit sichert.

2.3 Umfassende und praxistaugliche Neubewertung von Transparenzpflichten

KI-basierte Suchmaschinen oder Algorithmen ermöglichen das systematische Sammeln, Aufbereiten und Zweckentfremden von Informationen aus dem Internet. So können beispielsweise potenzielle Angriffsziele identifiziert und Drohnen programmiert werden. Vor diesem Hintergrund müssen die Transparenzpflichten für Betreiber kritischer Infrastrukturen zügig und ganzheitlich neu bewertet und angepasst werden. Bestehende Webangebote der Behörden oder von Open-Source-Quellen, die systematisch Leistungsdaten und / oder Geolokationen von kritischer Infrastruktur bereitstellen, müssen beschränkt / abstrahiert werden.

Es muss bei Portalen von Landes- oder Bundesbehörden grundsätzlich nachvollziehbar sein, wer Infrastrukturdaten abruft. Auch sollten deshalb Ausschreibungen und Verbändebeteiligungen in Zukunft nur der Branche und Stakeholder mit nachgewiesenem Interesse, nicht aber einer breiten Öffentlichkeit zugänglich gemacht werden, wenn diese sicherheitsrelevante Aspekte der Planung und Umsetzung von Vorhaben der kritischen Infrastrukturen zum Inhalt haben.

Sofern die Bereitstellung der Informationen durch kritische Infrastrukturen die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten

würde, sollte keine Pflicht zur Bereitstellung von Informationen nach den Informationsfreiheitsgesetzen der Länder bestehen (analog § 6a BSIG).

Schließlich sollten die möglichen Risiken der Transparenzpflichten auch Gegenstand der Nationalen Risikobetrachtung sein.

2.4 Möglichkeit der Strafverfolgung gemäß Strafgesetzbuch

Eingriffe in die Infrastrukturen der Energie- und Wasserversorgung soll analog zu Eingriffen in die Bahninfrastruktur gemäß § 315 StGB strafrechtlich geahndet werden können. Dies könnte eine abschreckende Wirkung entfalten.

2.5 Fehlende Umsetzung im Gesetzestext der Zweiwegekommunikation

Trotz einer klaren Begründung findet sich im eigentlichen Gesetzestext kein ausdrücklicher Passus zur institutionellen Verankerung einer Zweiwegekommunikation mehr.

Die Regelungen betreffen dabei vor allem die Meldepflichten der Betreiber (§§ 13 ff.) sowie die Aufsichtsfunktion der Behörden (§ 20 ff.).

Ein Mechanismus, der eine verpflichtende, systematische Rückmeldung der Behörden an Betreiber – etwa in Form von Lagebildern, Handlungsempfehlungen oder standardisierten Feedback-Schleifen – vorsieht, ist darin nicht enthalten. Damit reduziert sich die Kommunikation rechtlich auf ein Einbahnstraßensystem: Betreiber melden, Behörden empfangen und verarbeiten.

Die Betreiber sind jedoch aufgrund ihrer Verpflichtung zur Erstellung eigener Risikoanalysen gerade auf diese behördlichen Informationen angewiesen.

2.6 Ganzheitliche und praxistaugliche Weiterentwicklung des Rechtsrahmens für personelle Sicherheit

Bislang fehlt eine gesetzliche Grundlage, die definiert, wie Unternehmen rechtssicher überprüfen lassen können, ob Bewerbende, Mitarbeitende sowie Dienstleistende, die in sicherheitsrelevanten Unternehmenseinheiten – z.B. Konzernsicherheit, IT-Administration und IT-Sicherheit – tätig sind, zuverlässig und vertrauenswürdig sind und nicht im Geheimschutz oder vorbeugenden Sabotageschutz eingebunden sind.

Der BDEW spricht sich deshalb anschließend an den Vorschlag des BDI - Bundesverband der Deutschen Industrie e.V. dafür aus, ein Verfahren zu etablieren, das Rechtssicherheit für die Unternehmen schafft, die künftig unter den Anwendungsbereich der NIS-2-Umsetzung sowie der CER-RL-Umsetzung fallen und schlägt hierzu die Aufnahme einer freiwilligen Vertrauenswürdigkeitsüberprüfung vor. Diese Überprüfung muss jedoch auch zwingend innerhalb eines engen Zeitrahmens erfolgen, da der Fachkräftemangel nicht nur in der deutschen Wirtschaft dazu führt, dass in einem dynamischen Bewerbermarkt Entscheidungen schnell getroffen werden müssen. Eine solche Überprüfung muss durch staatliche Stellen durchgeführt werden.

Denkbar wäre daher auch eine Regelung, die ähnlich dem Atomrecht oder dem LuftSiG eine Überprüfung der Zuverlässigkeit, ggf. auch unter Entrichtung einer Verwaltungsgebühr, zulässt.

2.7 Klärung der Zuständigkeiten bei der Drohnenabwehr und Möglichkeit zur Beleihung der Betreiber

Es bedarf einer zügigen gesetzlichen Klärung über die Zuständigkeiten bei der hoheitlichen Aufgabe Drohnenabwehr sowie der Mitwirkungspflichten der Energie- und Wasserwirtschaft. Daraus darf sich keine gesetzliche Verpflichtung für die Betreiber kritischer Infrastrukturen zur Beschaffung und zum Betrieb von Systemen zur Drohnenabwehr ergeben. Betreiber kritischer Infrastrukturen können im Rahmen einer risikobasierten Bewertung ihrer Schutzbedarfe effektive, verhältnismäßige und wirtschaftliche Maßnahmen identifizieren und zwischen präventiven, baulichen oder BCM-Maßnahmen abwägen. Eine Beleihung der Betreiber zur Übernahme der Drohnenabwehr könnte dann sinnvoll sein, wenn andere Maßnahmen oder behördliche Fähigkeiten allein nicht ausreichen. Damit bliebe das staatliche Gewaltmonopol gewahrt. Damit die Beleihung praxistauglich wird, bedarf es einer gesetzlichen Klarstellung, dass Betreiber kritischer Infrastrukturen bei Abwehrhandlungen im Rahmen der Beleihung rechtlich wie hoheitlich handelnde Organe gestellt sind. Damit sollte eine staatliche Haftungsübernahme für Schäden verbunden sein, die aus rechtmäßigem Einsatz resultieren. Nur so können Betreiber die notwendigen Versicherungen abschließen und zugleich Planungssicherheit für Investitionen in Abwehrsysteme gewinnen. Eine entsprechende Anpassung des Luftverkehrsgesetzes, des Sicherheitsrechts sowie des Haftungsrechts ist daher unerlässlich, um Rechtssicherheit und Effektivität gleichermaßen zu gewährleisten.

2.8 Konfligierende Gesetzgebung zwischen Umwelt-, Straf- und KRITIS-Recht

Widersprüchliche und konfligierende gesetzliche Anforderungen an die KRITIS-Betreiber aus Umwelt- oder Strafrecht müssen unbedingt vermieden werden.

Der Fall etwa, dass die vollständige Entfernung bzw. Teilrückschnitt von Storchennestern auf 110 kV-Freileitungsmasten, die zu Kurzschlüssen innerhalb eines Systems führen und je nach Auftreten auch Todesfolge der Tiere nach sich ziehen kann, kann auch strafrechtliche Folgen für die Netzbetreiber haben. Die Entfernung oder der Eingriff in das Nest stellt eine Straftat nach §§ 71, 69 iVm § 44 BNatSchG dar. Dabei handelt es sich um ein Offizialdelikt, in dem behördlicherseits in jedem Fall ermittelt werden muss. Um einen Eingriff vornehmen zu dürfen, ist eine behördliche Genehmigung oder ein anderer Rechtfertigungsgrund erforderlich. Entstörungsmaßnahmen im Netz sind regelmäßig nicht vorab planbar, daher können hier notwendige Genehmigungen auch nicht weitläufig im Vorfeld eingeholt werden. Wenngleich davon auszugehen ist, dass eine Strafverfolgung aufgrund von Geringfügigkeit eingestellt würde, ist für die schnelle Abarbeitung ohne eine Prozessschleife zur Prüfung eventueller Straftatbestände hier eine Abkürzung im Sinne des Gesetzgebers. In diesem Sinne müssten andere Schutzgüter der schnellen Betriebswiederherstellung unterworfen werden – unter Berücksichtigung einer dokumentierten Güterabwägung und nachträglicher Mitteilung an die zuständigen Behörden.

Das KRITIS-Dachgesetz sollte daher eigens einen Rechtfertigungsgrund gegenüber anderen Rechtsnormen ausprägen, um diese konfligierende Gesetzgebung zu vermeiden.

2.9 Abgrenzung der Anforderungen von Behörden und KRITIS-Betreibern im Rahmen der Nationalen Risikoanalysen

Da die nationale Risikoanalyse auch als Grundlage zur Erstellung der Betreiber-Analysen genutzt werden soll und ggf. durch Prüfer sowie Auditoren bei Audits der Betreiber herangezogen werden könnte, sollte deutlich gemacht werden, dass die Maßnahmen der Gefahrenabwehr nur für die Gefahrenabwehrbehörden gelten und nicht im Rahmen der Betreiber-Risikoanalyse von den KRITIS-Betreibern selbst berücksichtigt werden muss.

Ferner sollte die Risikoanalyse auch feststellen, dass die schon heute bestehenden Risikobehandlungspläne der KRITIS-Betreiber als Risikoanalyse im Sinne der CER-RL zu verstehen sind.

2.10 Verbundunternehmen und technische Betriebsführer werden durch verschiedene Anforderungsregime auf Bundes- und Landesebene überfordert

Die zusätzliche Bestimmung von kritischen Anlagen, Schwellenwerten sowie Anforderungen durch die Bundesländer würde zu erheblichen Mehraufwänden bei Betreibern kritischer Anlagen führen. Viele dieser Betreiber haben entweder in mehreren Bundesländern kritische Anlagen, die kritischen Anlagen erstrecken sich über mehrere Bundesländer oder diese Betreiber übernehmen für Dritte in anderen Bundesländern die technische Betriebsführung. Auf die Dienstleistungen der technischen Betriebsführer sind hunderte kleine und meist kommunale Stadtwerke in Deutschland angewiesen. Durch das gleichzeitige Ansetzen verschiedener landesrechtlicher Regelungen droht, dass aufgrund des anfallenden Mehraufwandes die technischen Betriebsführer ihre Dienstleistung diesen kommunalen Stadtwerken nicht mehr wirtschaftlich anbieten können.

Besonders dramatisch wäre das gleichzeitige Anlegen von bundesrechtlichen und landesrechtlichen Regimen aber insbesondere für Verbundunternehmen, die neben bundesrechtlichen Regelungen etwa im Sektor Energie dann landesrechtliche Regelungen etwa für Wasser zu berücksichtigen hätten.

2.11 Behördliche Abstimmung bzgl. maritimen Infrastrukturen

Die Unternehmen mit maritimen Infrastrukturen fordern eine enge und umfassende Abstimmung zwischen den zuständigen Behörden BBK, BNetzA sowie dem BSH. Dabei sollte das BBK als federführende Behörde die speziellen Anforderungen und Besonderheiten des maritimen Bereichs als gleichwertigen und integralen Bestandteil in die übergreifende Risikoanalyse einbeziehen.

Die derzeit vorliegenden Analysen berücksichtigen maritime Aspekte bislang nicht in ihrer Komplexität.

Da maritime Risikofaktoren und Szenarien sich nicht eins zu eins auf andere Bereiche übertragen lassen, bedarf es einer eigenständigen, fachlich fundierten Betrachtung und einer systematischen Integration in die Gesamtstrategie.

Ein abgestimmtes Einvernehmen zwischen den Fachbehörden ist hierfür unerlässlich, um sicherzustellen, dass die jeweiligen Regelungen miteinander im Einklang stehen. Die Dringlichkeit dieser Koordination wird beispielhaft deutlich durch die Nebenbestimmungen der BSH-

Genehmigung für den Probebetrieb und deren Auswirkungen auf betrieblich notwendige Survey- und Sensorikmaßnahmen.

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik

Telefon: 030 / 300 199 - 1526

Mathias.Boeswetter@bdew.de