Der Schutz der kritischen Infrastruktur in herausfordernden Zeiten

Professor Dr. Martin Kment, LL.M. (Cambridge)*

Die Verbindungslinien zwischen nationalem und europäischem Recht lassen sich breitflächig in unserer Rechtsordnung nachweisen. Sie sind das (Zwischen-)Ergebnis eines fortschreitenden Integrationsprozesses, den Hans D. Jarass über Jahrzehnte mit großer Sachkunde rechtswissenschaftlich begleitet hat. Der Jubilar vollendet am 29.9.2025 sein 80. Lebensjahr. Bis heute interessiert ihn im Kontext der fortschreitenden Europäisierung des Rechts das Zusammenspiel der Normen, die Interaktion der Institutionen und die daraus erwachsenden, konkreten Konsequenzen für die Rechtsanwendung. Der vorliegende Beitrag ist Hans D. Jarass in herzlicher Verbundenheit und großer Dankbarkeit gewidmet. Er will den wissenschaftlichen Interessen des Jubilars nachspüren und sucht sich den Schutz kritischer Infrastrukturen als Exempel, um daran die Verzahnung von europäischem und nationalem Recht zu verdeutlichen. Ad multos annos, lieber Hans!

I. Erforderliche Wehrhaftigkeit

Die alten Gewissheiten gibt es nicht mehr; die Machtzentren der Welt verschieben sich. Im aufziehenden Sturm der Disruption ist Europa[1] neben außenpolitischen Herausforderungen und innenpolitischen Spannungen auch (weiteren) „hybriden Bedrohungen“[2] ausgesetzt. Es geht um nicht weniger als die Aufrechterhaltung der Versorgungssicherheit und mit ihr um den Schutz der kritischen Infrastruktur innerhalb der Europäischen Gemeinschaft. Wurden in jüngster Zeit mit der Sorge um kritische Infrastrukturen bislang insbesondere Cybergefahren in den Blick genommen,[3] weitet der europäische Normgeber sein Engagement nunmehr aus, um auch die *physische* Resilienz bedeutsamer Einrichtungen zu steigern, die die gesellschaftlichen Funktionen oder wirtschaftlichen Tätigkeiten innerhalb des Binnenmarkts aufrechterhalten.[4] Diese Einrichtungen kommen aus den Bereichen Energie, Verkehr, Finanzdienstleistung und Gesundheit. Auch die Versorgung mit Trinkwasser und Lebensmitteln soll gewährleistet werden, ebenso wie der Schutz der Abwassersysteme, der digitalen Infrastruktur und der öffentlichen Verwaltung.[5] Die einzelnen Sektoren sind nicht nur für sich genommen bisweilen sehr vulnerabel. Durch ihre gegenseitige Verzahnung können auch leicht Kaskadeneffekte im Zusammenspiel der Sektoren entstehen, die gegebenenfalls zu anderen Wirtschaftsbereichen übergreifen und in einer Katastrophe enden können. Der physische Schutz kritischer Infrastrukturen ist somit ein Projekt erheblichen Ausmaßes und von gesteigerter Priorität.

Aufgrund dieser Herausforderung hat die EU in der RL (EU) 2022/2557 (Critical Entities Resilience Richtlinie, im Folgenden: CER-RL) die Mitgliedstaaten in die Pflicht genommen, sich der Sicherungsaufgabe in Kooperation mit den betroffenen (privaten) Einrichtungsbetreibern anzunehmen. Erste Entwürfe für eine nationale Regelung – das KRITIS-Dachgesetz (KRITIS-E)[6] – sind jedoch nach dem Zerbrechen der „Ampelregierung“ dem Grundsatz der Diskontinuität[7] anheimgefallen. Da die Umsetzungsfrist für die europäischen Richtlinienvorgaben gem. Art. 26 CER-RL bereits am 17.10.2024 abgelaufen ist, dürfte der deutsche Gesetzgeber ohne großes Zögern mit einem neuen Gesetzgebungsverfahren beginnen. Es besteht die Hoffnung, dass er kritische

Erwägungen zum alten Gesetzentwurf[8] aufgreift und im anstehenden Gesetzgebungsverfahren berücksichtigt. Der Koalitionsvertrag, der eine „Architektur unserer Sicherheit“ in Deutschland zum erklärten Ziel der neuen Koalitionäre macht,[9] gibt hierzu jedenfalls Anlass.

II. Gefahrenlage

Um das erforderliche Abwehrsystem passgenau zu konzipieren, ist zunächst zu klären, welchen Risiken sich Deutschland und die EU zukünftig ausgesetzt sehen. Hier lassen sich zwei Bereiche ausmachen: Die Infrastruktur kann durch naturbedingte oder vom Menschen unmittelbar verursachte Krafteinwirkungen beeinträchtigt werden. An wirtschaftlich essenziellen Knotenpunkten wird dadurch deren Funktionsfähigkeit und damit auch die Erbringung von Dienstleistungen eingeschränkt.

1. Klimawandel und andere Umweltrisiken

Überschwemmungen, Erdbeben und Starkgewitter können desaströse Katastrophen auslösen. Doch selbst geringfügige Schäden verursachen signifikante Kaskadeneffekte.[10] Der menschenverschuldete Klimawandel ist maßgeblich dafür verantwortlich, dass sich diese Ereignisse häufen und bisweilen ein gewaltigeres Ausmaß annehmen. Die Überschwemmungen im Ahrtal oder in Süddeutschland belegen, dass sich auch Deutschland nicht in Sicherheit wähnen kann.[11] Bis zur Funktionslosigkeit wurden dort Trinkwasser- und Stromversorgung sowie Verkehrsmöglichkeiten beeinträchtigt.[12] Schäden in Milliardenhöhe sind entstanden. Die unzureichend gesicherte Infrastruktur wurde weitestgehend zerstört und ließ die Bevölkerung in ihrer Existenz bedroht und hilflos zurück.[13] Neben solch großen Naturkatastrophen droht eine häufig unerwähnte Gefahr von Substanzschäden durch Trockenperioden oder Winterstürme.[14] Insbesondere in der Transportbranche werden durch Substanzschäden sowohl Personen- als auch Güterverkehr erheblich beeinträchtigt.[15] Aber auch die sonstige Infrastruktur, wie die Energie- und Lebensmittelversorgung, erleidet akute und persistente Belastungsproben durch Umweltrisiken, denen zwingend begegnet werden muss.

2. Krieg

Neben umweltbedingten Gefahren gibt es auch menschliche Risikofaktoren: Sabotage, Terrorismus und Krieg.[16] Zwar ist die Bundesrepublik – soweit ersichtlich – in der jüngeren Vergangenheit noch von keinen schwerwiegenden Schädigungen dieser Art betroffen gewesen; im Jahr 2024 entfielen auf sie „lediglich“ drei der insgesamt 120 Anschläge in der EU.[17] Die Ereignisse um den Kupferdiebstahl vom 8.10.2022, der in weiten Teilen Norddeutschlands den Zugverkehr ausfallen ließ, nachdem unbekannte Täter Kabel der Steuerungsleitung der Deutschen Bahn in Nordrhein-Westfalen und Berlin mutwillig zerstört hatten,[18] verdeutlichen gleichwohl die Anfälligkeit der Verkehrsinfrastruktur. Sie geben einen Vorgeschmack auf Beeinträchtigungen, die vergleichbare oder tiefgreifendere Sabotageakte nach sich ziehen könnten. Den befürchteten Beeinträchtigungen ist grundsätzlich gemein, dass die Täter durch minimale Krafteinwirkungen („Nadelstiche“) einen größtmöglichen materiellen oder immateriellen Schaden herbeiführen wollen. Ihr Ziel ist es, Schwachstellen in der Sicherheitsarchitektur möglichst effizient auszunutzen, wozu sie mitunter modernste Technologien einsetzen.[19] Seit der Eskalation des russischen Angriffskriegs hat sich die Gefahrenlage in Europa spürbar zugespitzt: Regelmäßig „testet“ die russische Führung die Verteidigungsfähigkeit westlicher Unterstützer der Ukraine.[20] Auch werden Meereskabel für Strom und Kommunikation durch einzelne Schiffe der sog. „Schattenflotte“ in der Ostsee beschädigt[21] oder Zugverbindungen ins Visier genommen.[22] Dieses Aggressionspotenzial kann schnell auf andere Infrastrukturen in Europa umschlagen, schließlich sind – wie der Krieg in der Ukraine belegt – Infrastrukturen als Lebensadern des gesellschaftlichen Zusammenlebens beliebte Angriffsziele, insbesondere wenn es um Energie oder Telekommunikation geht.[23] Die attestierten Spannungen wurden durch die neue Regierung der Vereinigten Staaten von Amerika und deren Haltung gegenüber Europa (leider) verstärkt.[24] Es entsteht eine Instabilität der europäischen Verteidigungs- und Sicherheitsarchitektur und damit einhergehend eine potenzielle Lücke in den europäischen Versorgungsstrukturen. Man muss sich daher mit der Frage auseinandersetzen, ob die EU – und die Bundesrepublik im Besonderen – auf infrastrukturbezogene Angriffe ausreichend vorbereitet ist.[25]

III. Die CER-RL

1. Hintergrund und systematische Stellung innerhalb der europäischen Sicherheitsarchitektur

Die Verdichtung der „hybriden Bedrohungslage“ hat sich seit Jahrzehnten abgezeichnet.[26] Doch erst die jüngsten Symptome veranlassten die EU, ihr bestehendes Sicherheitssystem zu aktualisieren. Ursprünglich war es nur der Bekämpfung von Terrorismus gewidmet; nunmehr gilt die Aufmerksamkeit dem ganzheitlichen Schutz der „kritischen Infrastruktur“, den hohen Interdependenzen sowie den Kaskadeneffekten der versorgungsrelevanten Dienstleistungen, denn im europäischen Binnenmarkt wird ein hoher Schutzmaßstab zunehmend notwendiger.[27] Daher war es zwingend, dass die EU ihre Normsetzungskompetenz nutzte, um das Gesamtsystem an Verzahnungen der Binnenwirtschaft im europäischen Markt zu schützen.[28]

Zu Beginn ist im Jahr 2008 die RL 2008/114/EG (EKI-RL) in Kraft getreten,[29] die der Prävention, der Abwehrbereitschaft und der Reaktionsfähigkeit in Bezug auf terroristische Anschläge gegen kritische Energie- und Verkehrsinfrastruk-

turen galt.[30] Gefolgt ist später die Änderungs- und Aufhebungsrichtlinie RL (EU) 2022/2557 (CER-RL). Die aus dem Jahr 2022 stammende CER-RL entstand nach einer Revision der EKI-RL.[31] Die genannten Gefahrenursprünge haben sich zwar seit 2008 nicht wesentlich geändert, doch hat sich deren Eintrittswahrscheinlichkeit dramatisch erhöht.[32] Dies ist aber nicht der einzige Grund, warum eine Überarbeitung des europäischen Sicherheitsrechts in Angriff genommen wurde: Maßgeblich war auch, dass auf Grundlage der EKI-RL keine ausreichend kohärenten nationalstaatlichen Regelungen geschaffen wurden.[33] Zu große, unionsrechtlich gewährte Umsetzungsspielräume standen einem einheitlichen Ansatz im Wege. Insbesondere wurden zu wenige „europäische kritische Einrichtungen“ („EKI“) durch die Mitgliedstaaten ausgewiesen und an die (zu geringen) Ausweisungen zu weit divergierende nationale Schutzstandards geknüpft.[34] Nichtsdestotrotz wollte die Kommission an der Grundidee der EKI-RL festhalten, einen allgemeinen subsidiären Schutzstandard für Europa zu erarbeiten, mit sektorübergreifenden und -spezifischen Vorgaben sowie der Berücksichtigung aller Abhängigkeiten.[35] Sie verfolgt daher den Grundansatz der EKI-RL weiter, baut diesen jedoch durch strengere Maßstäbe und einen verbreiterten Anwendungsbereich der Richtlinie aus. Kompetenzrechtlich stützt sie sich dabei auf Art. 114 I AEUV, da sie mit einem ausgeweiteten Schutz kritischer Infrastrukturen die Grundbedingungen des europäischen Binnenmarktes gewährleisten will.[36]

2. Anwendungsbereich und Begrifflichkeiten der CER-RL

Entsprechend dem Gesetzgebungswillen erstreckt die EU den Anwendungsbereich der Schutzrichtlinie nicht mehr nur auf „kritische Einrichtungen, die von besonderer Bedeutung für Europa sind“ (vgl. Art. 17 f. CER-RL), sondern gem. Art. 1 I Buchst. b CER-RL vorsorglich auf alle, auch rein nationale „kritische Einrichtungen“ iSd Art. 2 Nr. 1 CER-RL. Wie bereits dargestellt,[37] stammen diese kritischen Einrichtungen nicht nur aus den Sektoren Energie und Transportwesen, sondern können in einer Vielzahl an Sektoren anzutreffen sein, vgl. Art. 2 Nr. 1 CER-RL in Verbindung mit dem Anhang. Bei den kritischen Einrichtungen kann es sich gem. Art. 2 Nr. 1 CER-RL um öffentliche oder private handeln; sie werden nach Art. 6 CER-RL von den Mitgliedstaaten selbst ermittelt.

Um europarelevante Einrichtungen weiterhin mit Nachdruck zu schützen, finden sich hierfür besondere Vorschriften in Art. 17 CER-RL: Als „kritische Einrichtungen, die von besonderer Bedeutung für Europa sind“ qualifizieren sich nur solche, die für mindestens sechs Mitgliedstaaten relevante Dienstleistungen erbringen. Dies ist eine Verschärfung der rechtlichen Anforderungen im Verhältnis zur früheren Rechtslage. Außerdem wird mit Inkrafttreten der CER-RL der „kritischen Einrichtung“ die Kategorie der „kritischen Infrastruktur“ (Art. 2 Nr. 4 CER-RL) gegenübergestellt. Anstatt alle materiellen und immateriellen Strukturen

anzusprechen, ist der Begriff der „kritischen Infrastruktur“ enger gefasst und betitelt nun ausschließlich den physischen Aspekt von Einrichtungen.[38] Gemeint sind körperliche (Teil-)Anlagen, Netze, Objekte oder Systeme, die für die Erbringung eines „wesentlichen Dienstes“ (Art. 2 Nr. 5 CER-RL) erforderlich sind. Ein solcher Dienst besteht, wenn er für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen sowie wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit, Sicherheit oder den Erhalt der Umwelt von entscheidender Bedeutung ist. Genau bei diesen Diensten muss die „Resilienz“ gesteigert werden. Letzteres ist gem. Art. 2 Nr. 2 CER-RL die Fähigkeit, bei tatsächlicher oder möglicher Beeinträchtigung der „wesentlichen Dienste“, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen.

Der physische Schutz der Einrichtungen und die Aufrechterhaltung der von ihnen zu erbringenden gesellschaftlichen Funktionen stehen im Mittelpunkt der CER-RL, nicht aber die Risiken durch Cyberangriffe; vgl. Art. 1 II CER-RL. Cybersicherheitsstrategien sind im Einklang mit RL (EU) 2022/2555 (NIS-2-RL) zu entwickeln, die einen mit der CER-RL kohärenten Ansatz verfolgt, um Effizienzen und Synergien zu ermöglichen.[39] Außerdem erstreckt sich die CER-RL nicht auf Einrichtungen, die im Zusammenhang mit der nationalen oder öffentlichen Sicherheit, Verteidigung oder Strafverfolgung stehen (Art. 1 VI CER-RL) und lässt auch die diesbezüglichen Zuständigkeiten der Mitgliedstaaten (Art. 1 V CER-RL) unversehrt. Sensible Informationen, die aus diesem Bereich herrühren, werden auf Grundlage der CER-RL ebenfalls nicht erhoben (Art. 1 VIII CER-RL); auch personenbezogene Daten sind gem. Art. 1 IX CER-RL im Einklang mit dem sonstigen, näher spezifizierten Unionsrecht zu schützen. Schließlich ist zu beachten, dass die EU die VO (EU) 2022/2554 (DORA-VO)[40] erlassen hat, um unmittelbar den Schutz der Informations- und Kommunikationstechnologien im Finanzsektor zu normieren; auch insofern kommt die CER-RL nicht zur Anwendung.

3. Architektur der CER-RL

Um den subsidiären Charakter der früheren EKI-RL fortzuführen, will die CER-RL nur dann eingreifen, wenn leistungsspezifisch noch keine vergleichbaren oder höheren Schutzmaßnahmen in den Mitgliedstaaten bestehen.[41] Daher wird gem. Art. 3 CER-RL eine Mindestharmonisierung vorgenommen, die es den Mitgliedstaaten freistellt, weitreichendere nationale Regelungen zu erlassen, um die Resilienz ihrer kritischen Infrastrukturen über das europäische Niveau hinaus zu steigern. Minimalziel der CER-RL ist die Etablierung eines mehrstufigen, aufeinander aufbauenden Verfahrens zur schrittweisen Resilienzsteigerung (Art. 4 ff. CER-RL) unter Einschluss staatlicher Stellen wie auch privater Einrichtungsbetreiber. Das Verfahren besteht aus einem erst-

maligen Ermitteln der Normadressaten, dem Ausarbeiten von Defiziten und Schutzmaßnahmen sowie der anschließenden Bewertung des Vorgehens. So können in einem nachgelagerten Informationsaustausch alle staatlichen und privaten Akteure ihre Erkenntnisse bündeln und von der Pluralität der Ideen profitieren. Hinzu treten regelmäßige Aktualisierungspflichten für nahezu alle getätigten Handlungen, um ein stets aktuelles Normengefüge zu schaffen. Verknappt könnte man davon sprechen, dass die Richtlinie in erster Linie Denk- und Handlungsanstöße initiiert, eigene staatliche Regelungen zu treffen und privatwirtschaftlich an der eigenen Resilienz zu arbeiten.

a) Stufe eins: Tätigwerden der Mitgliedstaaten

Grundstein des europäischen Schutzkonzepts ist gem. Art. 4 CER-RL eine nationale, politische Strategie zur generellen Verbesserung der Resilienz kritischer Einrichtungen. Sie ist von den Mitgliedstaaten im Anschluss an Konsultationsverfahren mit Interessenvertretern der betroffenen Sektoren zu entwickeln und weist gem. Art. 4 II CER-RL bestimmte Mindestelemente auf. Dazu gehört ua eine Ziel- und

Prioritätensetzung einschließlich eines Steuerungsrahmens, um diese Ziele und Prioritäten zu verwirklichen (Buchst. a, b), eine Beschreibung von erforderlichen Maßnahmen zur Verbesserung der Gesamtresilienz kritischer Einrichtungen (Buchst. c), von Verfahren zur Ermittlung dieser Einrichtungen (Buchst. d) und ihrer Unterstützung (Buchst. e) sowie zu behördlichen Koordinationsprozessen (Buchst. g). Die nationale Strategie stellt dann den Ausgangspunkt für eine nationale Risikobewertung nach Art. 5 CER-RL dar. Letztere umfasst breit angelegte Erkenntnisarbeiten auf Bundesebene, die alle denkbaren Sicherheitsrisiken erfassen und deren Wahrscheinlichkeit bewerten (Art. 5 II CER-RL). Hierbei sind auch sektorübergreifende und grenzüberschreitende Varianten einzubeziehen (Art. 5 I CER-RL). Als Orientierungshilfe bei der Erarbeitung der Risikobewertung sieht Art. 5 I CER-RL eine vorgeschaltete europäische Bewertung der Kommission vor, in der bereits einige wesentliche Dienste in den Wirtschaftssektoren aufgezählt sind.[42] Pro Sektor sind auch allgemeine und spezifische Informationen zu Resilienzmaßnahmen vorgesehen, die der Vor- und Nachsorge von Bedrohungen, Risiken oder Schwachstellen dienen (Art. 5 III CER-RL).

Daneben hat der Mitgliedstaat nach Art. 6 I–III CER-RL alle nationalen kritischen Einrichtungen, die wesentliche Dienste (Art. 2 Nr. 5 CER-RL) erbringen und die sonstigen Anforderungen des Art. 6 II CER-RL erfüllen, in einer Liste zu ermitteln. Hierbei ist den Mitgliedstaaten die Vorgehensweise grundsätzlich freigestellt, wobei die nationale Strategie und Risikobewertung zu berücksichtigen sind. Im Zentrum der Ermittlungsarbeit steht daher die Frage, ob die betrachtete Dienstleistung mit Wurzeln im Hoheitsgebiet des Mitgliedstaats eine erhebliche Störung nach Art. 7 I CER-RL auslösen kann. Die „kritischen Einrichtungen" hat der Staat dann über ihre Einstufung und die damit verbundenen Pflichten zu informieren (Art. 6 III CER-RL) und in der Aufgabenerfüllung zu fördern, wobei ihm sogar Subventionen zugunsten der kritischen Einrichtungen ermöglicht werden; Art. 10 CER-RL.

Während des dargestellten Prozesses bleibt die Kommission über die nationale Strategie und Risikobewertung informiert (Art. 4 III, 5 IV CER-RL) und erfährt gem. Art. 7 II CER-RL die wesentlichen Dienste, kritischen Einrichtungen und die zu ihrer Ermittlung eingesetzten Schwellenwerte; auch unterstützt die Kommission gem. Art. 6 VI CER-RL bei der Ermittlung der kritischen Einrichtungen. Dies gilt auch im Fall der Aktualisierung von Strategie, Risikobewertung und Ermittlung, die in einem Abstand von spätestens vier Jahren durchzuführen sind (Art. 4 II, III, 5 I 2, 6 V 1 CER-RL).

Um die Kommunikation zwischen allen Akteuren zu vereinfachen, führt die CER-RL den altbekannten Ansatz der EKI-RL aus dem Jahr 2008 fort: Von den Mitgliedstaaten ist eine nationale zentrale Anlaufstelle und mindestens eine zuständige Behörde für die Erfüllung der auferlegten Pflichten nach Art. 9 CER-RL zu benennen. Sie soll auch mit anderen Mitgliedstaaten und jeweiligen Cybersecurity-Behörden im Sinne der NIS-2-RL zusammenarbeiten (Art. 9 VI, Art. 11 CER-RL); so werden die Unionsvorgaben zum Schutz kritischer Infrastrukturen richtlinienübergreifend institutionell verschränkt. Die Anlaufstellen sind auch deshalb notwendig, da auch eine Meldepflicht von Sicherheitsvorfällen entsteht, die es gem. Art. 15 CER-RL zu koordinieren gilt. Zuletzt sollen nach Art. 21 CER-RL alle zuständigen Behörden Aufsichts- und Durchsetzungsmaßnahmen gegenüber den kritischen Einrichtungen durchsetzen können.

b) Stufe zwei: Verpflichtungen der kritischen Einrichtungen

aa) Kritische Einrichtungen

Die ermittelten kritischen Einrichtungen benennen gem. Art. 13 III CER-RL für ihren Betrieb Ansprechpartner und führen gem. Art. 12 CER-RL innerhalb von neun Monaten selbstständig eine individuelle, betriebsspezifische Risikobewertung durch. Grundlage für die Bewertungen sind gem. Art. 12 I CER-RL alle von den jeweiligen Mitgliedstaaten und der Kommission oder sonstigen Staaten erarbeiteten Unterlagen. Die Risikobewertung jeder kritischen Einheit legt überdies besonderen Wert auf die Abhängigkeit der eigenen Leistungsfähigkeit von den wesentlichen Diensten anderer kritischer Einrichtungen, selbst wenn diese einem anderen Sektor zuzuordnen sind, Art. 12 II CER-RL.

Durch diese breit angelegte Bewertung – in Verbindung mit sonstigen Unterlagen – sind gem. Art. 13 CER-RL Resilienzmaßnahmen zu treffen. Letzteres sind die konkreten, nach außen sichtbaren Schritte, die zur Verbesserung der Widerstandsfähigkeit der Dienstleistung ergriffen werden. Sie sollen verhältnismäßig sein

und sich speziell gegen Sicherheitsvorfälle wenden. Das kann gem. Art. 13 II iVm I CER-RL erreicht werden durch Erhöhung des physischen Schutzes, Prozessoptimierungen zur Abhilfe eines Sicherheitsvorfalls und die Schulung und Überwachung des Personals. In besonders sensiblen Bereichen kann sogar eine Zuverlässigkeitsprüfung von Mitarbeitern beantragt werden (Art. 14 CER-RL).

Kommt es trotz aller Vorsichtsmaßnahmen gleichwohl zu einem Sicherheitsvorfall oder ist eine erhebliche Störung eines wesentlichen Dienstes zumindest möglich, hat eine kritische Einrichtung dies gem. Art. 15 I, II CER-RL unverzüglich nach Kenntnisnahme, jedoch spätestens nach 24 Stunden, der zuständigen Behörde zu melden. Letztere antwortet wiederum so schnell wie möglich mit „sachdienlichen Folgeinformationen" und informiert zusätzlich die Öffentlichkeit nach pflichtgemäßem Ermessen, falls ein öffentliches Interesse daran besteht, Art. 15 IV CER-RL. Auch zuständige Behörden anderer Mitgliedstaaten werden gem. Art. 15 III CER-RL in Kenntnis gesetzt, falls grenzüberschreitende Aus-

wirkungen zu befürchten sind. Optional kann die betroffene Einrichtung im Anschluss, spätestens nach einem Monat, einen ausführlichen Bericht über alle bekannten Parameter erstellen und übermitteln.

bb) Kritische Einrichtungen mit besonderer europäischer Bedeutung

Die „kritischen Einrichtungen mit besonderer europäischer Bedeutung" werden in der CER-RL separat behandelt (Art. 17 CER-RL), obschon diese *en gros* keine anderen Pflichten treffen als „normale" kritische Einrichtungen. Die Resilienzmaßnahmen müssen auch bei den unionsweit bedeutsamen Einrichtungen stets verhältnismäßig sein, was allerdings umso leichter anzunehmen ist, je elementarer sich ein Dienst erweist. Zusätzlich wird nach Art. 18 CER-RL die Möglichkeit eröffnet, die Erfüllung der nationalen Pflichten durch eine Beratungsmission überprüfen zu lassen. Diese Mission ist der Kommission unterstellt und wird von ihr koordiniert.[43] Sie ist auf konstruktive Kritik ausgerichtet und besteht aus Sachverständigen aller betroffenen Staaten sowie aus Vertretern der Kommission selbst. Der Zweck ist, Unterstützung und produktive Hilfe zu liefern, keine Maßregelung. Die Mission soll die Risikobewertung, die Resilienzmaßnahmen, aber auch die Aufsichts- oder Durchsetzungsmaßnahmen bewerten, Defizite identifizieren und Verbesserungsvorschläge unterbreiten. Daher hat sie eine herausgehobene Stellung, vor allem mit besonderen Informationsrechten. Einen von ihr zu verfassenden Bericht bewertet wiederum die Kommission. Der Kreis schließt sich, indem die geprüften Einrichtungen diese Erwägungen dann implementieren.

c) Stufe drei: Anpassungen im Rahmen abgestimmter Zusammenarbeit

Die Kommission trifft koordinierende und normsetzende Entscheidungen, um das Gesamtgefüge des Resilienzschutzes zu optimieren. Im Besonderen sammelt sie Strategien (Art. 4 III CER-RL) und weist – wie dargestellt – durch Verordnung wesentliche Dienste aus (Art. 5 I 1 iVm Art. 23 CER-RL).[44] Zentrale Pflicht ist zudem das Sammeln und Konsolidieren der getroffenen Maßnahmen, um gem. Art. 13 V, VI CER-RL „best practices" herauszubilden. Dies versetzt die Kommission in die Lage, die Mitgliedstaaten und die kritischen Einrichtungen bei ihren Aufgaben zu unterstützen, Art. 20 CER-RL. Hierzu können auch bewährte Verfahren, Leitfäden und Methoden ausgearbeitet sowie grenzüberschreitende Schulungsmaßnahmen und grenzüberschreitende Übungen zur Überprüfung der Resilienz kritischer Einrichtungen entwickelt werden.

Gestärkt wird die interstaatliche Kommunikation, Kooperation und Koordination durch eine „Gruppe für die Resilienz kritischer Einrichtungen", Art. 19 CER-RL. Sie besteht aus Vertretern aller Staaten und der Kommission sowie gegebenenfalls aus speziellen Interessenvertretern. Sie soll die Kommission bei ihren Tätigkeiten unterstützen. Daneben wird sie zur Schnittstelle der zentralen Anlaufstellen hinsichtlich des Informationsaustauschs.

4. Zusammenfassung

Die CER-RL steht in einer Tradition mit der überkommenen Regelungstechnik der alten EKI-RL. Hierauf aufbauend will sie universell, aber doch feinmaschig ein ganzheitliches System schrittweise etablieren. Das erreicht sie, indem die kritischen Sektoren stark ausgeweitet werden. Es liegt dann jedoch vor allem an den Einrichtungen selbst, konkrete Vorschläge und Konzepte auf Grundlage staatlicher Vorgaben und Bewertungen erst zu entwickeln, dann umzusetzen. So entsteht die notwendig hohe Granularität in diesem sehr weitreichenden Regelungsgebiet des Infrastrukturschutzes. Vielversprechend, doch zeitlich noch weit entfernt, ist der angestrebte interstaatliche Vergleich. Der Diskurs aller Beteiligten wird die Einheitlichkeit beflügeln und die Akzeptanz stärken. Bis zu diesem Stadium werden Resilienzstandards aber nicht unmittelbar unionsrechtlich geklärt, so dass positive Effekte der CER-RL vorerst noch nicht spürbar sind. Im Besonderen werden private Unternehmen ihre Investitionen in Schutzmaßnahmen zu Beginn wohl auf ein Minimum beschränken wollen, bis die Aufsichtsmaßnahmen der zuständigen Behörden – oder die Beratungsmission – zu mehr Engagement führen werden und damit dem Infrastrukturschutz zu mehr Effektivität verhelfen.[45]

Der unionsrechtliche Regelungsansatz erzeugt ein aufeinander aufbauendes System von Strategien, Rechtsnormen und Risikoanalysen im Sinne eines fortwährenden Annäherungs- und Optimierungsprozesses. Allerdings ist das gewählte Konstrukt sehr zeit- und ressourcenintensiv und mit Blick auf die relevanten (neuen) Sektoren breit angelegt. So könnte es sich zu einem schleppenden und unübersichtlichen Bürokratiemonster entwickeln, welches in einer Flut von Berichtspflichten, Abstimmungsprozessen und Kooperationsschleifen zu ersticken droht, also das genaue Gegenteil von effektiver Gefahrenabwehr. Überdies ist zu befürchten, dass ein zu träges, abwartendes Vorgehen der involvierten Akteure gerade zu Beginn dazu führt, dass Regelungsunsicherheiten verbleiben, die den gewünschten Konkretisierungsprozess bzgl. der Schutzpflichten nicht richtig „anspringen“ lassen.

IV. Status quo des nationalen KRITIS-Schutzes

Das nationale Recht sieht den Gefahren für die eigene Infrastruktur nicht gleichgültig zu, obschon es eine Umsetzung der CER-RL bislang noch nicht gegeben hat. Der existierende Normenkanon teilt sich in solche des physischen und des digitalen Schutzes auf. Die digitale Netz- und Informationssicherheit (Cybersecurity) wird bundesrechtlich seit der NIS-1-RL[46] vor allem im BSIG[47] verankert. Das BSIG wird durch die BSI-KritisV[48] ergänzt, die bereits jetzt kritische Infrastrukturen sektorbezogen anhand von Grenzwerten bestimmt. Die §§ 8a ff. BSIG haben europäische Wurzeln und befassen sich primär mit Cybersicherheit: Wie auch von der noch nicht umgesetzten NIS-2-RL gefordert,[49] werden zugunsten der Cybersicherheit institutionelle Strukturen geschaffen (§ 8b BSIG) und Pflichten für die Betreiber der kritischen Infrastrukturen eingeführt (§§ 8a, 8c ff. BSIG). Hierzu gehören ebenso Meldepflichten wie auch technische und organisatorische Maßnahmen. Daneben finden sich spezialgesetzliche Regeln in §§ 11 Ia ff. EnWG, §§ 168 f. TKG, §§ 41 ff. AtG,[50] die vorrangig anzuwenden sind.

Im Gegensatz zur Cybersicherheit ist die physische Sicherheit in Deutschland bislang nur stiefmütterlich behandelt worden. Es fehlt insbesondere an einem zentralen Gesetz, das sich in Umsetzung der CER-RL einer breit angelegten, physischen Sicherheit annimmt. Eine der wenigen Normen, die dieses Anliegen bereits aufgreifen, ist § 2 II Nr. 3 ROG. Die planungsrechtliche Vorschrift erfasst den Schutz physischer Daseinsvorsorge in der Raumordnung und erhebt ihn zu einem öffentlichen Belang (Grundsatz der Raumordnung nach § 3 I Nr. 3 ROG). Hier sollen die jeweiligen Schwachstellen der Infrastruktur und deren Dienstleistungen erarbei-

tet und in behördlichen Entscheidungsprozessen berücksichtigt werden.[51] Ansonsten werden bundesrechtlich nur noch sektorspezifische Anlagen wie im EnWG, TKG oder der ÜNSchutzV geschützt; dies rührt von der (alten) EKI-RL her. Daneben schützt das landesrechtliche Sicherheitsrecht allgemein,

ohne Rücksicht auf die speziellen Anforderungen der Einrichtungen, und wird teilweise durch speziellere Einzelregelungen des landesrechtlichen Katastrophenschutzes ergänzt.[52]

V. Die Aufgaben des künftigen Gesetzgebers

Der deutsche Gesetzgeber hat die Umsetzungsfrist der CER-RL, die gem. Art. 26 CER-RL bis zum 17.10.2024 lief, verstreichen lassen. Grund für die Verzögerung sind im Wesentlichen die Turbulenzen der 20. Bundesregierung, wohl aber auch die brisante außenpolitische Lage, in der sich die Bundesrepublik Deutschland bis heute befindet.[53] Aufgrund dieser Umstände wäre eine Umsetzung aber umso wichtiger:[54] Weder die (Außen-)Politik noch die Umweltrisiken nehmen auf staatliche Versäumnisse Rücksicht.

1. Allgemeines: Kompetenz, Grundkonzept, Begrifflichkeiten

Aufgrund des steigenden Umsetzungsdrucks spricht einiges dafür, dass die neue Bundesregierung den Schutz der kritischen Infrastruktur wieder schnell auf ihre Agenda setzen wird und in diesem Zuge auf die Vorarbeiten der Vorgängerregierung zumindest aufbauen dürfte. Der letzte Gesetzentwurf – der KRITIS-E[55] – aus dem Jahr 2024 hatte schließlich die wesentlichen Inhalte der CER-RL umgesetzt, auch wenn man über Details sicherlich streiten kann.[56] Obschon der 2024er-Entwurf der Diskontinuität zum Opfer gefallen ist, dient er nachfolgend als Referenzpunkt, um an ihm Herausforderungen zu verdeutlichen, denkbare Umsetzungsoptionen aufzuzeigen und vermeidbare Fehlsteuerungen zu benennen.

a) Gesetzgebungskompetenz und einheitliches Schutzregime

Eine erste Herausforderung für den Gesetzgeber ist die verfassungsrechtliche Ausgangslage – konkret die Gesetzgebungskompetenzen, die er vorfindet. Bislang hat sich der Bund, wenn es um den Schutz kritischer Infrastrukturen ging, primär auf seine Kompetenz für das Recht der Wirtschaft (Art. 74 I Nr. 11 GG) berufen und die Erforderlichkeit einer bundesweiten Wirtschaftseinheit nach Art. 72 II GG mit der Verhinderung von Wettbewerbsverzerrungen im Bundesgebiet begründet.[57] Diese Argumentation ist allerdings erkennbar zu wirtschaftslastig. Sie übersieht die Bezugspunkte zum Katastrophenschutz und der Gefahrenabwehr, die beide in den Kompetenzbereich der Länder fallen.[58] Selbst wenn man ergänzende Bundeskompetenzen aus den Bereichen Luftverkehr (Art. 73 I Nr. 6 GG), Eisen- und Schienenbahn (Art. 73 I Nr. 6a, 74 I Nr. 23 GG), Telekommunikation (Art. 73 I Nr. 7 GG), Schifffahrt (Art. 74 I Nr. 21 GG) oder Gesundheit (Art. 74 I Nr. 19 GG) hinzunimmt und diese durch Annexkompetenzen auch auf die Gefahrenabwehr auszudehnen sucht,[59] bleibt es schlussendlich bei einem bunten Strauß an bundes- und landesrechtlichen (Rest-)Kompetenzen, die eine bundesweit einheitliche (Voll-)Regelung zum Schutz kritischer Infrastrukturen nicht erlauben.[60] Diese verfassungsrechtliche Ausgangslage provoziert Ineffizienzen und leistet einem Regelungsdschungel Vorschub, der sich aufseiten des Gesetzesvollzugs mit nicht unverminderter Härte fortsetzt, wenn der Gesetzgeber nicht die Kraft zum Zurückstutzen des Wildwuchses findet: Nach dem ursprünglichen KRITIS-E sollten neben den vielen zuständigen Landesbehörden auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie außerdem eine gemeinsame Meldestelle (vgl. § 32 BSIG-E) und noch eine zweistellige Zahl weiterer besonderer Bundesbehörden, wie die BNetzA, das Eisenbahnbundesamt oder das Bundesamt für Seeschifffahrt und Hydrographie (vgl. ausführlich § 3 II KRITIS-E) in ihren jeweiligen Spezialgebieten am Konzert der Exekutivakteure teilnehmen. Dies mündet unter anderem auch in breiten Abstimmungsorgien beim Erlass von Rechtsverordnungen (vgl. § 4 IV KRITIS-E) und schürt berechtigte Ängste betroffener Unternehmen, sich im komplexen Kosmos der Zuständigkeiten zu verirren.[61]

Es gibt gute Argumente, dem kompetenzrechtlich zersplitterten Regelungsgegenstand der „KRITIS“ Rechnung zu tragen, indem man den Weg eines Artikelgesetzes einschlägt, um so die thematische Auffächerung nachzuzeichnen. Diesen Ansatz wollte die Vorgängerregierung bei der Umsetzung der NIS-2-RL ebenfalls gehen.[62] Andererseits hätte die Wahl eines „Dachgesetzes“ den Vorteil, durch einen großen Regelungsansatz für alle angesprochenen Bereiche (Telekommunikation, Energie, Verkehr etc.) regulatorische Grundlinien vorzugeben. Diese könnten dann bereichsspezifisch durch Spezialgesetze oder Rechtsverordnungen konkretisiert und – im Zuge des unionsrechtlich eingeforderten, schrittweisen „Lernens“ – fortentwickelt werden, um sich auf homogener Basis einem bestmöglichen Schutzniveau

anzunähern. Diese Vorteile scheinen den Gesetzgeber bei seinen Umsetzungsbemühungen zur CER-RL überzeugt zu haben, unternahm er doch Bemühungen, beim Schutz physischer Infrastrukturen diese Systematik zu wählen.[63] Egal welchem Modell man näher steht, so ist doch eines klar: Die gleichzeitige Verwendung *beider Modelle* zur Umsetzung des Unionsrechts überzeugt nicht. Insbesondere der Dachgesetz-Ansatz spricht vielmehr dafür, Cybersecurity und physischen Schutz in einem Gesetzeswerk zusammenzuführen, nicht nur, weil sie thematisch eng zusammengehören, sondern weil die unionsrechtlichen Vorgaben eine parallele Regelungsstruktur aufzeigen, die synchronisiert, wenn nicht gar miteinander verschmolzen werden könnte.[64] Die unionsrechtliche Auffächerung in zwei unterschiedlichen Richtlinien hindert den deutschen Gesetzgeber jedenfalls nicht an einer nationalen Zusammenführung, die zusätzlich der Gefahr von Inkonsistenzen entgegenwirkt.[65]

Unabhängig davon, welchen Weg der Gesetzgeber beschreitet, wird es wohl keinen Königsweg geben, denn das föderale Kompetenzgefüge wird sich absehbar zum Bremsklotz des Schutzes kritischer Infrastrukturen mausern. Theoretisch könnte eine Grundgesetzänderung für Entlastung sorgen, deren Umsetzung aber fernliegend ist. Praktisch wird man allenfalls überlegen können, durch einen Staatsvertrag der Länder – wie im Glücksspielrecht –[66] Vereinheitlichungen zu vereinbaren oder jedenfalls durch Mustergesetzgebungen – wie im Bauordnungsrecht –[67] die landesrechtliche Normierung anzuleiten. Gelingt nicht einmal dies, könnte es förderlich sein, auf Bundesebene eine (informelle) „Empfehlung“ zu erarbeiten, die gerade leistungsschwächeren Landesministerien als Orientierungshilfe bei ihren Regelungsbemühungen dienen könnte. Erfahrungen zur Abweichungsgesetzgebung nach Art. 72 III GG zeigen, dass eine Vielzahl von Landesgesetzgebern durchaus dankbar ist, bundesrechtliche Regelungen vorzufinden und nicht selbst erlassen zu müssen.[68]

b) Begriffsbestimmungen

Im Kontrast zu den Gesetzgebungsbefugnissen dürfte es dem nationalen Gesetzgeber deutlich einfacher fallen, die Begrifflichkeiten der Zwillingsregelungen zum Cyber- und physischen Schutz einheitlich zu wählen. Dies wird auch dabei helfen, durch gegenseitige *spill-over*-Effekte Rechtserkenntnisse innerhalb der Schutzregime auszutauschen. Bei der Umsetzung der Richtlinien ist es außerdem möglich und durchaus sachgerecht, die Termini des Unionsrechts dem national etablierten Sprachgebrauch anzupassen, selbst wenn dies die Arbeit mit den unionsrechtlichen Grundlagen in der Rechtspraxis etwas erschweren mag. Die bisherigen Normierungsansätze wiesen bereits in diese Richtung: So wurden etwa die „wesentlichen Dienstleistungen“ (Art. 2 Nr. 5 CER-RL) zu „kritischen Dienstleistungen“ (§ 2 Nr. 4 KRITIS-E; § 2 Nr. 24 BSIG-E) und die „kritischen Einrichtungen“ nach Art. 2 Nr. 1 CER-RL mutierten zu „kritischen Anlagen“ (§ 2 Nr. 3 KRITIS-E; § 2 Nr. 22 BSIG-E), wobei ihnen „Betreiber kritischer Anlagen“ (§ 2 Nr. 1 KRITIS-E) an die Seite gestellt wurden; die „kritische Einrichtung“ der CER-RL wurde somit aufgeteilt in die Anlage als feste Installation auf der einen und den letztlich verantwortlichen Betreiber auf der anderen Seite.[69] Entsprechende Anpassungen sollte der Gesetzgeber bei einem erneuten Normierungsversuch in Erwägung ziehen.

2. Ermittlungs- und Auswertungsarbeit

Das unionsrechtliche Normenskelett ist darauf angelegt, dass in den Mitgliedstaaten vielfältige Ermittlungs- und Auswertungsprozesse angestoßen werden.[70] So sind neben den schützenswerten Dienstleistungen auch die kritischen Einrichtungen zu bestimmen. Letztere werden wiederum auf der Basis nationaler Risikoanalysen und -bewertungen schrittweise herausgefiltert. Nur so wird sichergestellt, dass die ermittelten kritischen Einrichtungen auch tatsächlich für die zu schützenden Dienstleistungen erheblich sind. Die identifizierten Anlagenbetreiber führen im Anschluss ihrerseits Risikoanalysen und -bewertungen durch, um (gegebenenfalls mit staatlicher Hilfe) auf die sachgerechten Resilienzmaßnahmen zu schließen.

Vor dem Hintergrund des spezifischen Risikos einer jeden kritischen Einrichtung ist so auch die Grundlage gelegt, Resilienzpläne zu erarbeiten, die helfen, effektiv mit Angriffen bzw. Störungen umzugehen. Einzelne dieser Verfahrensschritte werden regelmäßig wiederholt, um den Schutzstandard neuen Erkenntnissen und Entwicklungen anzupassen.

Der Erfolg dieser sehr komplexen Abfolge von Verfahrensschritten hängt maßgeblich davon ab, dass die jeweiligen Analysen und Bewertungen mit präzisen Vorgaben angeleitet werden. In Anlehnung etwa an eine Umweltprüfung nach §§ 39 ff. UVPG müsste durch den Gesetzgeber klar definiert werden, welcher Struktur die einzelnen Prüfungen zu folgen haben, auf welchen sachlichen und räumlichen Prüfraum sie sich beziehen und welche Faktoren untersucht werden sollen. Auch wenn sich bestimmte Standards erst im Verlauf der Untersuchungen herauskristallisieren sollen, können die in festen Zeitfenstern wiederkehrend durchzuführenden Verfahrensrunden nur Konkretisierungsschritte, nicht aber Ersatz eines anfänglich erforderlichen, staatlichen Steuerungsrahmens sein: Ein Mindestmaß an Standards, Grenzwerten und relevanten Merkmalen wird der Normgeber schon zu Beginn liefern müssen, um die Entwicklung in die rechten Bahnen zu lenken. Der Gesetzentwurf zum KRITIS hatte insofern bereits gesetzliche Mindestvorgaben kombiniert mit einer Verordnungsermächtigung vorgesehen; vgl. etwa §§ 5, 11, 12 KRITIS-E. Eine hinreichende Rahmensetzung war dies allein allerdings noch nicht.

Klare gesetzliche Vorgaben sind außerdem nötig, um bei der Auswahl der kritischen Infrastrukturen neben der abstrakten Definition der relevanten Anlagentypen eine Korrektur bzw. Ergänzung der identifizierten Gruppe im Einzelfall zu ermöglichen. Voraussetzungslose staatliche Einordnungen darf es nicht geben; § 5 III 2 KRITIS-E sah deshalb zumindest eine Anlehnung an allgemeine, gesetzlich definierte Gesichtspunkte bei Einzelfallentscheidungen vor. Des Weiteren müssen die privaten Anlagenbetreiber bei den von ihnen verlangten Risikoanalysen und -bewertungen an die Hand genommen werden. Eigenständig können sie ua nicht feststellen, welche Gefahren konkret relevant sind und welche systemrelevanten Interdependenzen in Bezug auf das eigene Unternehmen bzw. aus Sicht von Drittunternehmen mit ihnen existieren. Als wirtschaftlich Leidtragende der europäischen Schutzinitiative werden sie sonst im Zweifel geringere Ausgaben bevorzugen und ihre Schutzbemühungen eher am unteren als am oberen Ende der Ausgabenskala ansiedeln.

Der ehemalige § 5 I, II KRITIS-E zeigte bei der Ermittlung kritischer Dienstleistungen erste gute Ansätze zur Ausrichtung der Prüfung, übertrug den wesentlichen Teil der Aufgabe allerdings auf den Verordnungsgeber; ähnlich sahen es §§ 11, 12 KRITIS-E vor. Diese Regelungstechnik ist grundsätzlich nicht zu beanstanden, muss jedoch die rechtlichen Anforderungen des Wesentlichkeitsgrundsatzes beachten.[71] Außerdem ist ganz allgemein zu fordern, dass die Festlegung von Standards, Richt- und Schwellenwerten, Kennziffern, Merkmalen, Methoden und Kategorien sowie alle sonstigen Ausrichtungen von Ermittlungs- und Bewertungstätigkeiten im Kontext des Schutzes kritischer Infrastrukturen möglichst unter Hinzuziehung der betroffenen Unternehmen erfolgen

sollte.[72] Letztgenannte spielen im Kreislauf der Resilienzoptimierung eine eigenständige Rolle (etwa bei der Risikoanalyse und -bewertung; vgl. auch § 12 KRITIS-E) und beeinflussen damit den Gesamtprozess ohnehin; außerdem verfügen sie bisweilen über wertvolles Spezialwissen, das vorzeitig erhoben und normativ verarbeitet werden kann. Insofern hatte der ehemalige Gesetzentwurf zum KRITIS Potenziale verschenkt. Umgekehrt ist darauf zu achten, die Zahl der Einflussnehmenden nicht zu stark anwachsen zu lassen. Verfahrensbeteiligungen und Gestaltungsbefugnisse sollten nur solchen Stellen und nur in dem Umfang zukommen, wie sie über erhöhte Fachkenntnis verfügen.[73] Dies gilt etwa für Fachaufsichtsbehörden, die in bestimmten Infrastrukturbereichen bereits jetzt den Schutz physischer Infrastruktur beaufsichtigen (vgl. etwa die Flugaufsicht).[74] Eine Überfrachtung der Normsetzung mit

unzähligen Beteiligungs- und Einvernehmensregeln ist demgegenüber dysfunktional und schleppend.[75] Ebenfalls aus Gründen der Qualitätssteigerung sollten branchenspezifische Anforderungen, die von den Betreibern selbst definiert werden, Vorrang vor der staatlichen Festsetzung erhalten. Letztere ist erst dann angezeigt, wenn die Anlagenbetreiber keine Vorgaben entwickeln oder solche erkennbar unzureichend sind. Bundesweite Vereinheitlichungen durch Rechtsverordnungen, die auf der Basis von Resilienzvorgaben der Wirtschaft erarbeitet werden, sind ebenfalls begrüßenswert.[76]

Schädlich ist es demgegenüber, wenn es in den einzelnen Bundesländern abweichende Standards gibt oder wenn das Verhältnis zwischen dem allgemeinen KRITIS-Ansatz und spezielleren Fachgesetzen ungeklärt bleibt;[77] vor allem unbeschränkte „Öffnungsklauseln" für sonstige rechtliche Vorgaben (vgl. etwa § 6 I 2 KRITIS-E) aus Bund und Ländern fördern allenfalls die Unübersichtlichkeit der Regelungsmaterie. In der Regel bietet es sich an, den – bereits funktionstüchtigen – Fachgesetzen den Vorzug zu erteilen (vgl. etwa §§ 6–11 LuftVG); dies vermeidet auch Doppelbelastungen.[78] Jedenfalls sollten großzügige Abschichtungsregeln die Prüfungsleistungen nach dem KRITIS-Ansatz erleichtern, um Ressourcen und Zeit zu sparen.[79]

Schließlich bietet es sich an, aus dem verspäteten deutschen Umsetzungsprozess der Richtlinien einen Vorteil zu ziehen. Es liegt nahe, die schon bestehenden Umsetzungsstrategien anderer Mitgliedstaaten, die vor der Bundesrepublik Deutschland die unionsrechtlichen Richtlinienvorgaben zum Schutz der Infrastrukturen umgesetzt haben, genau zu analysieren, um von den Erfahrungen der weiter fortgeschrittenen Rechtsordnungen zu lernen. Ein Benchmarking innerhalb des europäischen Rechtsraums wird zukünftig ohnehin unumgänglich sein.[80] Die Definition des Schutzstandards kritischer Infrastrukturen (Resilienzniveau), der untrennbar mit den beschriebenen Vorgaben zu den unterschiedlichen Prüfungen verbunden ist, ist nämlich ein marktrelevantes Faktum. Um Wettbewerbsverzerrungen innerhalb der EU zu vermeiden und insbesondere Beeinträchtigungen der Wettbewerbsfähigkeit deutscher Unternehmen abzuwenden, wird der Blick über die Grenze nachdrücklich geboten sein.[81]

3. Verantwortung und Finanzierung

Der Schutz kritischer Infrastrukturen erfordert die Zusammenarbeit zwischen staatlichen Stellen und privaten Anlagenbetreibern.[82] Auf dem breiten Kooperationsfeld begegnen sie sich an unterschiedlichen Stellen, bisweilen überschneiden sich auch ihre Aktivitäten. Der Gesetzgeber sollte daher die Umsetzung der unionsrechtlichen Richtlinienbestimmungen nutzen, um die Verantwortungsbereiche zwischen beiden Akteuren herauszuarbeiten.[83] Dies ist insbesondere für die Privatwirtschaft notwendig, um die finanzielle Belastung des Schutzes kritischer Infrastrukturen besser ermitteln zu können. Hier besteht aufgrund des unionsrechtlich provozierten, herantastenden Konkretisierungsansatzes ohnehin ein großes Maß an Verunsicherung bezüglich der konkret zu ergreifenden, finanziell relevanten Schutzmaßnahmen.[84] Sicherlich werden die Betreiber kritischer Infrastrukturen aus eigenem Antrieb die für sie erforderlichen Schutzmaßnahmen gerne übernehmen,[85] gleichwohl aber weitergehende Maßnahmen kritisieren, die gesellschaftlich angezeigt, ökonomisch für sie jedoch unrentabel sind.[86]

Der KRITIS-Entwurf aus dem Jahr 2024 hatte die finanzielle Belastung der voraussichtlich 1.400 Betreiber kritischer Einrichtungen mit einem ungefähren Aufwand von jährlichen 500 Mio. EUR geschätzt.[87] Daneben rechnete der Gesetzgeber mit einem einmaligen Aufwand von 1,7 Mrd. EUR.[88] Obschon die finanzielle Belastung der privaten Betreiber kritischer Infrastrukturen damals wie heute potenziell erheblich ist, nutzte der frühere Entwurf zum KRITIS nicht die unionsrechtlich eröffnete Möglichkeit des Art. 10 I 2 CER-RL, betroffene Anlagenbetreiber finanziell zu unterstützen. Er bürdete ihnen lediglich Lasten auf, obschon die kritischen Infrastrukturen ihrer Natur nach für die Versorgungssicherheit der gesamten Bevölkerung wie auch die öffentliche Sicherheit des Staats elementar sind. Aus der gesamtgesellschaftlichen Bedeutung der Schutzmaßnahmen dürfte sich daher die Rechtfertigung für eine finanzielle Beteiligung des Staates leicht ableiten lassen,[89] zumal der neu eingeführte Art. 143h GG für ein solches finanzielles Engagement des Staates gerade geschaffen wurde.[90]

Bleibt die staatliche Finanzspritze allerdings aus, werden sicherheitsrelevante Investitionen im Bereich der kritischen

Infrastrukturen voraussichtlich schnell unter Effizienzdruck geraten, welcher der Bedeutung der Aufgabe nicht gerecht wird.[91] Es ist insbesondere zu befürchten, dass die betroffenen Anlagenbetreiber die weitgehend offene und bisweilen noch unspezifische Anforderungslage an Schutzmaßnahmen nutzen werden, um Minimallösungen zu fahren.[92] Immerhin liefert ihre Einbindung in den Prozess der Risikoermittlung einen Hebel, um das eigene Engagement ökonomischen Zwängen anzunähern. Die im Fluss befindliche Konkretisierung von Schutzmaßnahmen schwächt dabei auch die staatliche Kontrollfunktion, die einer verhaltenen Investitionsbereitschaft beim Schutz kritischer Infrastrukturen nur wenig entgegensetzen kann.[93] Auch um Wettbewerbsverzerrungen zu verhindern, sollte der Gesetzgeber die Chance eines zweiten Anlaufs zur Umsetzung der CER-RL nutzen, um sich finanziell an den Kosten der Sicherung der deutschen Infrastruktur zu beteiligen. Es würde die erforderliche Kooperationsbereitschaft der Wirtschaft in jedem Fall signifikant steigern.

4. Meldungen und KI-gestützte Digitalisierung

Das unionsrechtlich eingeforderte Herantasten an die Sicherheitsstandards beim Schutz kritischer Infrastrukturen erzwingt einen regen Austausch unterschiedlichster Informationen. Hierzu gehören auch die bereits geschilderten Berichtspflichten von öffentlichen Stellen und Betreibern kritischer Infrastrukturen.[94] Für manche sind derartige Berichtspflichten nicht ganz neu: Es bestehen im Luftsektor bereits jetzt spezielle Meldepflichten, wie bei sicherheitsrelevanten Vorfällen gegenüber der BAF.[95] Einige dieser Anlagenbetreiber haben ihre bisherigen Berichtspflichten optimiert und zeigen daher ein großes Interesse, diese in das KRITIS-Verfahren einzubringen.[96] Obschon das Anliegen auf den ersten Blick verständlich ist, sollte der Gesetzgeber eine Variationsbreite bei Berichten und Meldungen nicht zulassen. Vielmehr muss das primäre Anliegen sein, alle Arten der Kommunikation in einheitlichen Formaten, am besten elektronisch, erstellen zu lassen.[97] Dies ermöglicht es, die übermittelten Daten optimal digital zu erfassen und auszuwerten. Damit geht einher, dass es nicht mehr nötig sein sollte, als Anlagenbetreiber Meldungen oder Berichte bei mehr als einer Stelle einzureichen. Eine Digitalisierung der Datenverarbeitung – insbesondere unter Einsatz Künstlicher Intelligenz – dürfte es vielmehr erlauben, von der Erst-Empfängeradresse ausgehend automatisch weitere relevante Adressaten zu ermitteln und diesen unmittelbar die eingetroffenen Informationen zuzuleiten. Ein fortgeschrittener Grad der digitalen Verarbeitung dürfte für einen erheblichen Abbau von Bürokratie sorgen, Ressourcen auf staatlicher wie auch privater Seite einsparen und damit mögliche Nachteile des Wirtschaftsstandorts Deutschland verhindern. Zielpunkt muss eine Informationsübertragung per App sein.

Darüber hinaus dürfte der Einsatz Künstlicher Intelligenz helfen, in den gewonnenen Daten Muster und Häufungen zu erkennen[98] und so den Schutz kritischer Infrastrukturen möglichst kosteneffizient bei maximaler Wirkung zu betreiben. Flankierend könnten die Resilienzmaßnahmen der Anlagenbetreiber als Maßnahmen von besonderem öffentlichen Interesse aufgewertet werden,[99] um eine erleichterte Durchsetzung zu ermöglichen.

VI. Resümee

Die Anstrengungen der EU fallen nicht ohne Grund in eine weltpolitisch herausfordernde Zeit. Im Kampf gegen den Klimawandel, militärische Bedrohungen und Sabotageakte will sich die Union als resilient und handlungsfähig präsentieren. Die ersten Schritte wurden auf der europäischen Ebene mit Richtlinien zur Cybersicherheit und dem physischen Schutz kritischer Infrastrukturen gegangen. Nun liegt es an den Mitgliedstaaten, die unionsrechtlichen Impulse effektiv und effizient in das nationale Rechtsregime zu überführen. Ein erster Umsetzungsversuch ist der staatsrechtlichen Diskontinuität anheimgefallen. Auf ihm

lässt sich aber aufbauen und mit einigen Korrekturen eine überzeugende Umsetzung für Deutschland finden.

---

* Der Autor ist geschäftsführender Direktor des Instituts für Umweltrecht der Universität Augsburg und Inhaber des Lehrstuhls für Öffentliches Recht und Europarecht, Umweltrecht und Planungsrecht. Der Beitrag ist auf dem Bearbeitungsstand vom 28.7.2025; zu diesem Zeitpunkt waren alle Internetfundstellen abrufbar.

1 BVerfGE 89, 155 (181 ff.) = NJW 1993, 3047; Streinz/Pechstein, 3. Aufl. 2018, EUV Art. 1 Rn. 12.

2 Bundesregierung, Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, 13.7.2022, S. 16; CDU, CSU und SPD, Koalitionsvertrag 2025, Nr. 11 ff.

3 RL (EU) 2016/1148 v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-1-RL).

4 RL (EU) 2022/2557 v. 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der RL 2008/114/EG des Rates (CER-RL), Erwgr. 2 f.

5 Vgl. zu Einzelheiten Anlage 1 zur RL (EU) 2022/2557 (CER-RL).

6 BT-Drs. 20/13961 (KRITIS-E).

7 Stern/Sodan/Möstl StaatsR/Kau, 2. Aufl. 2022, § 43 Rn. 91 f.; Dürig/Herzog/Scholz/Kersten, 106. EL 2024, GG Art. 76 Rn. 116.

8 S. ausf. unter V. mit einer Auseinandersetzung zu den Stellungn. zum RefE vom 21.12.2023.

9 CDU, CSU und SPD, Koalitionsvertrag 2025, Nr. 48 f.

10 Vgl. GFZ Helmholtz-Zentrum für Geoforschung, New Multi-HAzard and MulTi-RIsK Assessment MethodS for Europe, https://cordis.europa.eu/project/id/265138.

11 DOI:10.5445/IR/1000171441; DOI:10.5445/IR/1000135730, S. 14 f.

12 DOI:10.5445/IR/1000135730, S. 28; DOI:10.5445/IR/1000171441, S. 21 ff.

13 DOI:10.5445/IR/1000135730, S. 25 f.; DOI:10.5445/IR/1000171441, S. 15 f.

14 DOI:10.5445/IR/1000143470.

15 DOI:10.5445/IR/1000135730, S. 30; Mühr/Kubisch/Marx/Stötzer/Wisotzky/Latt/Siegmann/Glattfelder/Mohr/Kunz, CEDIM Forensic Disaster Analysis „Dürre & Hitzewelle Sommer 2018 (Deutschland)“ Report No. 1.

16

BT-Drs. 20/15096, 1.

17 Vgl. Europol, Tendenz- und Lagebericht über den Terrorismus in der Europäischen Union (TE-SAT), 2024.

18 Tagesschau, Keine Sabotage, sondern Gier v. 28.7.2023, vgl. https://www.tagesschau.de/investigativ/bahn-ausfall-sabotage-kabel-diebstahl-100.html.

19 Europol, TE-SAT, 2024, S. 10.

20 S. etwa Merkur, Zwischenfall über der Ostsee: Putins Kriegsflugzeug von Nato-Jets gestoppt v. 17.5.2024, vgl. https://www.merkur.de/politik/putin-kriegsflugzeug-nato-f-16-jets-polen-ukraine-krieg-zwischenfall-ostsee-zr-93058385.html.

21 S. zdfheute, Russlands „hybrider Krieg" – Putins Plan: Die Gefahr der Schattentanker v. 22.1.2025, vgl. https://www.zdf.de/nachrichten/politik/ausland/putin-schattenflotte-tanker-krieg-ostsee-100.html; Fischer/Rust DVBl 2025, 742.

22 S. SZ, Geplante Anschläge auf Güterverkehr v. 14.5.2025, vgl. https://www.sueddeutsche.de/politik/sabotage-gueterverkehr-brandpakete-dhl-reul-russland-agenten-geheimdienst-li.3252534?reduced=true.

23 Tagesschau, Russland bombardiert Energienetze und Gasförderung v. 7.3.2025, vgl. https://www.tagesschau.de/ausland/europa/ukraine-krieg-luftangriffe-100.html.

24 v. Daniels/Mair, SWP-Studie 3, Februar 2025, S. 5 ff.

25 Hierauf reagiert der Koalitionsvertrag 2025, S. 3958 ff.

26 Flohn, Zeitschrift für Erdkunde, 1941 Heft 1/2, S. 13 (14 ff.); anstatt vieler Europol, TE-SAT, 2024, S. 11 f.

27 KOM(2004) 702 endg., 3; Tagung R 10679/2/04 REV 2, S. 3 f.; KOM(2005) 576 endg., S. 2 ff.

28 RL (EU) 2022/2557 (CER-RL), Präambel; BT-Drs. 20/13184, 91.

29 RL 2008/114/EG (EKI-RL) v. 8.12.2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, Art. 13.

30 RL 2008/114/EG (EKI-RL), Erwgr. 1, 5.

31 Kommission SWD(2019) 308 endg., 19 ff.

32 Kommission SWD(2019) 308 endg., 3.

33

RL (EU) 2022/2557 (CER-RL), Erwgr. 2; Kommission SWD(2019) 308 endg., 19.

34 Kommission SWD(2019) 308 endg., 25 f.; RL (EU) 2022/2557 (CER-RL), Erwgr. 3.

35 Kommission SWD(2019) 308 endg., 35; RL (EU) 2022/2557 (CER-RL), Erwgr. 2 f.

36 RL (EU) 2022/2557 (CER-RL), Präambel; Calliess/Ruffert/Korte, 6. Aufl. 2022, AEUV Art. 114 Rn. 2.

37 Siehe oben I.

38 Kommission SWD(2019) 308 endg., 35; RL (EU) 2022/2557 (CER-RL), Erwgr. 9; RL 2008/114/EG (EKI-RL), Erwgr. 5; KOM(2005) 576 endg., 8.

39 RL (EU) 2022/2555 v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS-2-RL), Erwgr. 30 f.

40 VO (EU) 2022/2554 v. 14.12.2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der VO 1060/2009/EG, 648/2012/EU, VO 600/2014/EU, 909/2014/EU und VO (EU) 2016/1011 (DORA-VO).

41 RL 2008/114/EG (EKI-RL), Erwgr. 9 f.; Kommission SWD(2019) 308 endg., 34.

42 Delegierte VO (EU) 2023/2450 der Kommission v. 25.7.2023 zur Ergänzung RL (EU) 2022/2557 (CER-RL).

43 BT-Drs. 20/13961, 53.

44 Dies ist bereits geschehen: vgl. oben III. 3. a).

45 Becker IR 2024, 270 (272 f.).

46 S. RL (EU) 2016/1148 (NIS-1-RL), dies ist die Vorgängerregelung der NIS-2-RL.

47 Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik, G. v. 17.12.1990, BGBl. 1990 I 2834 (BSI-Errichtungsgesetz – BSIG).

48 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, VO v. 22.4.2016 (BGBl. 2016 I 958) (BSI-Kritisverordnung – BSI-KritisV).

49 S. oben III. 2.

50 BT-Drs. 20/13961, 37; BT-Drs. 16/11967, 10.

51

NK-ROG/Kümper, 2019, ROG § 2 Rn. 53.

52 Eisenmenger NVwZ 2023, 1203 (1204).

53 CDU, CSU und SPD, Koalitionsvertrag 2025, Nr. 3962 ff.

54 Fischer/Rust DVBl 2025, 742.

55 BT-Drs. 20/13961. Mit Fokussierung auf maritime Infrastruktur s. dazu Fischer/Rust DVBl 2025, 742.

56 Becker IR 2024, 270 (272 f.); iE folgend bspw.: Deutsche Industrie- und Handelskammer (DIHK), Stellungnahme zu dem KRITIS-E, S. 2.

57 BT-Drs. 20/13961, 34.

58 BVerfGE 3, 407 (433 f.) = BeckRS 1954, 30700512; BayVerfGH NVwZ-RR 2012, 665 (667); Becker NJW-Beil. 2024, 50 Rn. 5.

59 S. Eisenmenger NVwZ 2023, 1203 (1205).

60 Fischer/Rust DVBl 2025, 742 (745).

61 Verband der Internetwirtschaft eV (ECO), Stellungnahme, S. 7; DIHK, Stellungnahme, S. 4; Verband kommunaler Unternehmen eV (VKU), Stellungnahme, S. 11.

62 BT-Drs. 20/13184, 92 f.

63 BT-Drs. 20/13961, 32.

64 Trotz gesehener Notwendigkeit der Vereinfachung sollten unterschiedliche Normen bei weitgehend gleichen Regelungen der Meldestellen geschaffen werden: §§ 8, 18 KRITIS-E, BT-Drs. 20/13961, 51 f. und 62; § 8b BSIG bzw. § 32 BSIG-E, BT-Drs. 20/13184, 187.

65 EuGH C-217/97, ECLI:EU:C:1999:395 = NVwZ 1999, 1209 – Kommission/Deutschland.

66 BayVerfGH NJOZ 2015, 1970 Rn. 141 ff. = NVwZ 2016, 137 Ls. = BayVBl 2016, 81; Eisenmenger NVwZ 2023, 1203 (1206); Verband der Automobilindustrie eV (VDA), Stellungnahme, S. 5; Bundesverband der Deutschen Industrie eV (BDI), Stellungnahme, S. 9.

67 So zB die Musterbauordnung – MBO, November 2002, zuletzt geändert durch Beschluss der Bauministerkonferenz v. 26./27.9.2024.

68

Meßerschmidt UPR 2008, 361 (367); Kloepfer ZUR 2006, 338 (339). Es ist nur ein vereinzeltes Nutzen der Möglichkeit feststellbar, vgl. Deutscher Bundestag, Nutzung der Abweichungskompetenz nach Art. 72 III GG, Sachstand WD 3 – 3000 – 157/18, S. 4 ff.

69 BT-Drs. 20/13961, 39.

70 S. ausf. und zu den nachf. Ausführungen bereits oben III. 3. a) und b).

71 BVerfGE 20, 150 (157 f.) = NJW 1966, 1651; BVerfGE 49, 89 (125 f.) = NJW 1979, 359; Dürig/Herzog/Scholz/Grzeszick, 106. EL, GG Art. 20, V. Gewaltenteilung, Rn. 96, 114.

72 VKU, Stellungnahme, S. 8 f.; VDA, Stellungnahme, S. 6.

73 Arbeitsgemeinschaft Deutscher Verkehrsflughäfen eV (ADV), Stellungnahme, S. 6.

74 Exemplarisch in §§ 2 ff. LuftSiG, §§ 19 f. AtomG.

75 Der Entwurf zum KRITIS war demgegenüber ein abschreckendes Bsp. Die §§ 5 I 2, 11 VIII 2, 12 III 2 KRITIS-E verwiesen alle auf § 4 IV, V KRITIS-E, der eine Vielzahl von Verfahrensbeteiligten benennt.

76 Die frühere Entwurfsfassung zum KRITIS sah demgegenüber in § 14 II 1 KRITIS-E lediglich ein Vorschlagsrecht für branchenspezifische Resilienzstandards vor.

77 VKU, Stellungnahme, S. 12, 23; VDA, Stellungnahme, S. 5; Deutscher Verein des Gas- und Wasserfaches eV (DVGW), Stellungnahme, S. 2.

78 ADV, Stellungnahme, S. 5.

79 Kment NVwZ 2024, 1609 (1614); Beckmann/Kment/Kment, 6. Aufl. 2023, UVPG § 39 Rn. 32 ff; Battis/Krautzberger/Löhr/Battis, 15. Aufl. 2022, BauGB § 2 Rn. 12.

80 VDA, Stellungnahme, S. 3.

81 Bertschek/Bünstorf/Cantner/Häussler/Schmidt/Welter, Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands, 2025, S. 9 (23, 27); Streinz/Trute/Pilniok, 3. Aufl. 2018, AEUV Art. 179 Rn. 17; Calliess/Ruffert/Ruffert, 6. Aufl. 2022, AEUV Art. 179 Rn. 11.

82 Stüer/Beckmann BauR-HdB/Beckmann, 6. Aufl. 2025, Rn. 7750 ff. mwN für das Kooperationsprinzip im Umweltrecht.

83 VKU, Stellungnahme, S. 2, 19 f.; Arbeitsgemeinschaft Stoffspezifische Abfallbehandlung eV (ASA), Stellungnahme, S. 2; Allianz für Sicherheit in der Wirtschaft eV (ASW), Stellungnahme, S. 2; Unabhängige Partnerschaft KRITIS (UP), Stellungnahme, S. 2.

84

Deutsches Verkehrsforum eV (DVF), Stellungnahme, S. 5; Deutsche Krankenhausgesellschaft (DKG), Stellungnahme, S. 21 f.; Deutsche Bahn AG (DB AG), Stellungnahme, S. 5; VKU, Stellungnahme, 28 f.; ADV, Stellungnahme, S. 7 f.

85 Vgl. ADV, Stellungnahme, S. 7.

86 Becker IR 2024, 270 (272); UNITI Bundesverband EnergieMittelstand eV (UNITI), Stellungnahme, S. 5.

87 BT-Drs. 20/13961, 4 und 36.

88 BT-Drs. 20/13961, 4 und 36.

89 Zum Energiesektor: Mitteilung der Kommission – Leitlinien für staatliche Umweltschutz- und Energiebeihilfen 2014 – 2020, ABl. 2014 C 200/01, 37; ADV, Stellungnahme, S. 7 f.

90 BT-Drs. 20/15096, 2 f., 9 f. und 13.

91 VKU, Stellungnahme, S. 22.

92 Becker IR 2024, 270 (272).

93 Bereits in der Forderung einer unternehmerischen Risikoakzeptanz erkennbar: VKU, Stellungnahme, S. 20.

94 S. dazu die obigen Ausführungen unter III. 3.

95 ZB in Art. 4 VO (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates v. 3.4.2014 über die Meldung, Analyse und Weiterverfolgung von Ereignissen in der Zivilluftfahrt, zur Änderung der VO (EU) Nr. 996/2010 des Europäischen Parlaments und des Rates und zur Aufhebung der RL 2003/42/EG des Europäischen Parlaments und des Rates und der VO (EG) 1321/2007 und VO (EG) 1330/2007 der Kommission.

96 ADV, Stellungnahme, S. 6 f.; Bundesverband der Deutschen Luftverkehrswirtschaft (BDL), Stellungnahme, S. 21.

97 BDL, Stellungnahme, S. 21; BDI, Stellungnahme, S. 14.

98 Schoch/Schneider/Hornung, 6. EL 2024, VwVfG § 35a Rn. 36; Wagner, Legal Tech und Legal Robots – Der Wandel im Rechtsmarkt durch neue Technologien und künstliche Intelligenz, 2018, S. 23.

99 Vgl. dazu Stüer/Beckmann BauR-HdB/Beckmann, 6. Aufl. 2025, Rn. 2196.