cyberintelligence.institute

MesseTurm | Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.
Tel.: + 49 69 505034 602
Mail: info@cyberintelligence.institute
Web: https://cyberintelligence.institute

Prof. Dr. Dennis-Kenji Kipker

Research Director cyberintelligence.institute
Mail: dennis.kipker@cyberintelligence.institute

Frankfurt am Main, 27. November 2025

Schriftliche Stellungnahme

zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz) vom 03.11.2025

BT-Drs. 21/2510

Über das cyberintelligence.institute (CII)

Das cyberintelligence.institute fungiert als Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanke sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Inhaltsverzeichnis

A. Vorbemerkung und zusammenfassende fachliche Einordnung

Kritische Infrastrukturen – die zentralen Versorgungs- und Funktionssysteme unseres Gemeinwesens – sind seit Jahren einer erheblich zunehmenden Gefährdungslage ausgesetzt. Die Zahl und Intensität von Angriffen auf Energie- und Wasserversorgung, Verkehrs- und Kommunikationsnetze sowie öffentliche Verwaltungsstrukturen haben deutlich zugenommen. Sabotageakte gegen Umspannwerke, Angriffe auf Bahninfrastruktur, IT-basierte Störungen kommunaler Verwaltungsleistungen und systematische Ausspähungen mittels Drohnentechnologie zeigen, dass abstrakte Risikoannahmen längst in konkrete sicherheitsrelevante Ereignisse umgeschlagen sind. Diese Entwicklungen sind Ausdruck einer hybriden Bedrohungslage, die durch staatliche und nichtstaatliche Akteure gleichermaßen befeuert wird.

Auch die deutschen Sicherheitsbehörden und das Parlamentarische Kontrollgremium haben wiederholt auf die erhebliche Zunahme nachrichtendienstlicher, cyberbasierter und physischer Angriffe hingewiesen. Nach der aktuellen Wirtschaftsschutzstudie des Branchenverbands BITKOM gaben im Jahr 2025 rund 87 % der Unternehmen an, von Datendiebstahl, Spionage oder Sabotage betroffen gewesen zu sein; der volkswirtschaftliche Schaden belief sich auf 289,2 Mrd. Euro. Diese Daten unterstreichen, dass der Schutz kritischer Infrastrukturen nicht nur ein technisch-operatives, sondern ein gesamtstaatlich sicherheitspolitisches Erfordernis ist.

Parallel dazu bestehen erhebliche Regelungslücken: Während im Bereich der digitalen Infrastruktur mit den IT-Sicherheitsgesetzen 1.0 und 2.0 bereits erste Regelungen geschaffen wurden, unterliegt die physische Infrastruktur bislang jedoch keinen eigenständigen Schutzvorgaben. Um diesen Befund zu beheben und europaweit ein kohärentes Schutzniveau zu schaffen, hat die Europäische Union im Jahr 2022 die Richtlinien (EU) 2022/2555 (NIS-2) und (EU) 2022/2557 (CER) erlassen, die den Schutz Kritischer Infrastrukturen sowohl im physischen als auch im digitalen Bereich stärken sollen. Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Resilienz gegenüber Naturgefahren, Terroranschlägen und Sabotage zu erhöhen, während die NIS-2-Richtlinie die Cybersicherheitsanforderungen auf weitere Sektoren und Betreiber ausdehnt. Beide Instrumente verfolgen ausdrücklich das Ziel eines einheitlichen, sektorenübergreifenden Schutzstandards – physisch wie digital.

Gleichwohl wurde die Umsetzungsfrist der CER-Richtlinie vom 18. Oktober 2024 überschritten, ohne dass ein konsistentes, zusammenführendes Regelwerk vorgelegt wurde. Das nun vorliegende KRITIS-Dachgesetz bleibt hinter den europäischen Anforderungen zurück und adressiert zentrale Herausforderungen nur unzureichend. Es gelingt insbesondere nicht, die erforderliche Verzahnung von digitaler und physischer Resilienz herzustellen, obwohl viele KRITIS-Betreiber zugleich von beiden Richtlinien erfasst werden. Die Folge sind potenzielle Doppelstrukturen, divergierende Melde- und Nachweispflichten sowie ein erheblicher Verwaltungsaufwand, der Ressourcen bindet, die für den tatsächlichen Schutzbedarf benötigt werden. Ein integriertes KRITIS-Dachgesetz, das physische und digitale Schutzanforderungen kohärent bündelt, ist jedoch ein wesentlicher Baustein einer umfassenden Sicherheitsstrategie gegen hybride Bedrohungen und Voraussetzung dafür, dass Deutschland seiner Verantwortung

zum Schutz seiner kritischen Infrastrukturen tatsächlich gerecht werden kann; nur ein solches konsistentes und einheitliches Gesamtgefüge vermag die Resilienz Kritischer Infrastrukturen nachhaltig zu stärken und den bestehenden Bedrohungen angemessen zu begegnen.

Im Lichte dessen, dass die Umsetzung in nationales Recht bereits seit geraumer Zeit möglich und geboten ist, weist der vorgelegte Entwurf weiterhin eine Reihe von Schwächen und Unklarheiten auf. Fachliche Hinweise und Kritikpunkte sind bislang nur eingeschränkt aufgegriffen worden. In der Folge finden sich im aktuellen Gesetzesentwurf in weiten Teilen die bereits bekannten Problemlagen wieder. Mit dem Anspruch, die Resilienz kritischer Infrastrukturen in Deutschland nachhaltig zu erhöhen und diese gegenüber aktuellen wie zukünftigen hybriden Bedrohungen angemessen zu schützen, ist dieser Zustand nur schwer vereinbar.

Im Einzelnen äußert sich die in dieser Stellungnahme dargelegte Kritik wie folgt:

- **Unangemessen kurze Fristen:** Sowohl das Gesetzgebungsverfahren als auch die Ausarbeitung der konkretisierenden Rechtsverordnung haben sich weiter verzögert, während der im Entwurf vorgesehene Stichtag für Betreiber kritischer Anlagen unverändert im Juli 2026 verbleibt. Damit reduziert sich der reale Zeitraum, in dem sich KRITIS-Betreiber auf die anstehende Registrierung vorbereiten können, deutlich.

- **Unzureichende Einbeziehung der öffentlichen Verwaltung:** Die öffentliche Verwaltung – einschließlich wesentlicher Teile der Bundes-, Landes- und Kommunalverwaltungen – bleibt weiterhin weitgehend vom Anwendungsbereich ausgeschlossen. Dies führt zu einem fragmentierten Schutzniveau. Die im KRITIS-Sektor „Staat und Verwaltung“ verorteten Infrastrukturen sollten jedoch denselben Resilienzanforderungen unterliegen wie Anlagen privater Betreiber; andernfalls verbleiben gerade staatliche Strukturen in einem vermeidbaren physischen Gefährdungsbereich.

- **Fehlende materiell-konkrete Resilienzanforderungen:** Der vorliegende Entwurf enthält bislang kaum materielle Vorgaben dazu, welche konkreten Resilienzmaßnahmen Betreiber kritischer Anlagen zu ergreifen haben; konkrete, unmittelbar aus dem Gesetz ableitbare Handlungsanweisungen für KRITIS-Betreiber fehlen somit weitestgehend. Im Mittelpunkt stehen überwiegend Zuständigkeits- und Verordnungsermächtigungen, also die Frage, welche Behörden künftig durch Rechtsverordnung Mindestverpflichtungen festlegen dürfen. Damit wird der Beginn substantieller Anforderungen auf einen späteren Zeitpunkt verschoben, an dem die noch ausstehenden Rechtsverordnungen erlassen sind. Ob die künftig vorgesehenen Mindeststandards tatsächlich zu einer spürbaren Erhöhung der Resilienz kritischer Anlagen und Systeme führen, lässt sich auf Grundlage des Entwurfs nicht beurteilen.

- **KRITIS-Resilienzstrategie:** Eine nationale KRITIS-Resilienzstrategie sollte zeitlich der Einführung regulatorischer Verpflichtungen für KRITIS-Betreiber vorausgehen. Um den betroffenen Unternehmen frühzeitig Klarheit und Planungssicherheit zu ermöglichen, ist es zudem sachgerecht, den Rückgriff auf Rechtsverordnungen auf das notwendige Maß zu beschränken und die wesentlichen Vorgaben möglichst unmittelbar im Gesetz selbst zu verankern.

- **Uneinheitliche Behörden- und Aufsichtsstrukturen:** Die Verteilung der Zuständigkeiten zwischen BBK, BSI, Fachaufsichten und Landesbehörden ist unklar und birgt das Risiko divergierender Vollzugspraxis. Zudem fehlen Regelungen für einen einheitlichen, strukturierten Datenaustausch und eine zentralisierte Meldestelle.

- **Meldeverfahren ohne ausreichende Entlastungs- und Rückmeldekomponenten:** Die Meldepflicht nach § 18 droht aufgrund unklarer Abgrenzungen und weiterhin parallel bestehender Meldewege zu erheblichem Aufwand zu führen. Ein strukturierter Rückkanal – etwa in Form von Lagebildern, Warnhinweisen oder Empfehlungen – fehlt bislang.

- **Weitreichende Ausnahmebefugnisse:** Die vorgesehenen Ausnahme- und Befreiungsmöglichkeiten in § 22 schwächen den Charakter des Gesetzes als Mindeststandard erheblich und eröffnen strukturelle Schutzlücken gerade in besonders sicherheitsrelevanten Bereichen.

- **Zu geringe Harmonisierung mit der NIS2-Umsetzung:** Trotz inhaltlicher Schnittmengen bestehen weiterhin erhebliche Divergenzen zwischen der NIS2-Umsetzung und dem KRITIS-DachG, die sich in der Praxis als problematisch erweisen. Unterschiedliche Begriffsverwendungen sowie abweichend ausgestaltete Anforderungen erschweren eine konsistente Betroffenheitsprüfung und führen zu einer vermeidbaren zusätzlichen Komplexität.

- **Unklare Begriffe und unbestimmte Kriterien:** Mehrere Begriffsbestimmungen bleiben unpräzise. Dies schafft Rechtsunsicherheit und erschwert die praktische Anwendung.

- **Unterdimensionierter Bußgeldrahmen:** Die vorgesehenen Bußgeldhöhen erreichen keine ausreichende Steuerungswirkung, insbesondere im Vergleich zu NIS2-relevanten Sanktionsrahmen.

Überdies bleiben die Angaben zum Erfüllungsaufwand (E.) insbesondere mit Blick auf die Wirtschaft weiterhin unzureichend, da finanzielle Belastungen für Betreiber kritischer Anlagen derzeit nicht belastbar quantifiziert werden und im Wesentlichen auf spätere Rechtsverordnungen verschoben sind.

B. Zu den Vorschriften im Einzelnen

- **Zu § 2 KRITIS-DachG-E (Begriffsbestimmungen, hier: insb. anlagenbezogener Ansatz):**

  In den Begriffsbestimmungen des § 2 bleibt unberücksichtigt, dass sich die Resilienz kritischer Dienstleistungen nicht auf die jeweilige Anlage im engeren Sinne beschränkt. Zahlreiche vor- und nachgelagerte Produkte und Dienstleistungen – etwa Logistik-, IT-, Wartungs- oder Zulieferleistungen – sind für die Aufrechterhaltung des kritischen Dienstes zwingend erforderlich und bilden faktisch Teil der „kritischen Kette". Diese Leistungen sind jedoch in der Regel sektorenübergreifend organisiert und werden vom Regelungsgehalt des KRITIS-Dachgesetzes derzeit nicht erfasst. Aus Resilienzperspektive wäre daher ein Paradigmenwechsel geboten: weg von der isolierten Betrachtung einzelner Anlagen hin zu einer systemischen Betrachtung der für den Betrieb notwendigen Gesamtkette an Aufgaben und Dienstleistungen. Nur wenn auch diese abhängigen und unterstützenden Leistungen in geeigneter Weise berücksichtigt und abgesichert werden, kann das angestrebte Schutzniveau für kritische Dienstleistungen tatsächlich erreicht werden. In diesem Zusammenhang fällt auf, dass der Entwurf auf eine eigenständige Legaldefinition „Kritischer Infrastrukturen" verzichtet und den Regelungsfokus im Wesentlichen auf „kritische Anlagen" verengt. Aus unions- und systematischen Gründen sollte der Begriff „Kritische Infrastruktur" jedoch im Gesetz selbst definiert und dabei im Einklang mit der CER-Richtlinie verstanden werden – also als Gesamtheit der für die Erbringung wesentlicher Dienstleistungen maßgeblichen Objekte, Anlagen, Systeme und Netze. Eine solche Klarstellung würde die Systematik des Gesetzes schärfen und verdeutlichen, dass es nicht um den punktuellen Schutz einzelner Objekte, sondern um die Resilienz gesamter Versorgungs- und Funktionssysteme geht.

- **Zu § 2 Nr. 10 KRITIS-DachG-E (Begriffsbestimmungen, hier „Einrichtungen der Bundesverwaltung"):**

  In § 2 werden Definitionen im Hinblick auf die betroffenen kritischen Anlagen sowie kritischen Dienstleistungen getroffen. Die in § 2 Nr. 10 gewählte Begriffsbestimmung der „Einrichtungen der Bundesverwaltung" greift indes deutlich zu kurz. Erfasst wird lediglich ein kleiner Ausschnitt der tatsächlichen Bundesverwaltung; sämtliche nachgeordneten Behörden bleiben außen vor. Zur Bundesverwaltung zählen jedoch laut einer allgemeinen Definition (https://www.bpb.de/kurz-knapp/lexika/politiklexikon/17259/bundesverwaltung/) grundsätzlich alle „Behörden und Einrichtungen des Bundes, die mit dem Vollzug von Bundesaufgaben betraut sind". Mit der lückenhaften Definition des § 2 Nr. 10 werden nicht nur die einem Ressort nachgeordneten Bundesbehörden (z. B. Bundesober- und Bundesmittelbehörden) ausgeblendet, sondern auch die mittelbare Bundesverwaltung (insbesondere bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts). Insbesondere dort werden in vielen Fällen kritische Dienstleistungen erbracht oder zentrale Unterstützungsfunktionen für die Funktionsfähigkeit des Bundes wahrgenommen.

  Wird dieser Bereich nicht in den Anwendungsbereich des KRITIS-DachG einbezogen, entstehen systematische Schutzlücken und ein uneinheitliches Resilienzniveau innerhalb

der Bundesverwaltung. Wenn Resilienz und Sicherheit des Bundes tatsächlich ganzheitlich gestärkt werden sollen, müssen daher sämtliche relevanten Behörden und Einrichtungen – einschließlich der nachgeordneten und mittelbaren Bundesverwaltung – in die Definition einbezogen werden.

- **Zu § 3 KRITIS-DachG-E (Zuständige Behörde; behördliche Zusammenarbeit):**

  § 3 sieht eine Aufteilung der Zuständigkeiten zwischen dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe als zentraler Anlaufstelle, weiteren Fachbehörden des Bundes und – für bestimmte Betreiber, Dienstleistungen und Sektoren – Behörden der Länder vor. Die Einbeziehung der Länder in die Umsetzung wird von Unternehmen ambivalent bewertet: Einer potentiell größeren Nähe zu den Betreibern und damit erleichterten Austausch- und Kooperationsprozessen steht die vielfach geäußerte Befürchtung gegenüber, dass unterschiedliche Landeszuständigkeiten zu einer uneinheitlichen Behördenpraxis und divergierenden Anforderungen führen. Sofern an der vorgesehenen Aufteilung der Zuständigkeiten zwischen Bundes- und Landesebene festgehalten wird, sollte diese daher so konkret wie möglich ausgestaltet werden, damit klare Zuständigkeitsabgrenzungen bestehen und insbesondere eine bundesweit einheitliche Handhabung – etwa durch gemeinsame Leitlinien, abgestimmte Vollzugshilfen und koordinierte Aufsichtspraxis – gewährleistet ist.

- **Zu § 4 KRITIS-DachG-E (Geltungsbereich; Sektoren; Verordnungsermächtigung):**

  Der KRITIS-Sektor „Staat und Verwaltung“ ist im vorliegenden Entwurf bedauerlicherweise nach wie vor nicht angemessen berücksichtigt. In § 4 ist dieser Bereich weiterhin vollständig ausgeklammert. Des Weiteren fehlt eine hinreichende Einbeziehung der Kommunalverwaltungen sowie der Behörden der Länder. Diese Stellen erbringen jedoch Dienstleistungen, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen gravierenden Folgen für das Gemeinwesen führen kann. Infolgedessen bleiben zentrale Teile des KRITIS-Sektors „Staat und Verwaltung“ ungeregelt, obwohl viele Kommunen nicht über ausreichende Ressourcen für eine durchgehende Überwachung ihrer Sicherheitsinfrastrukturen verfügen. Angesichts zahlreicher Angriffe auf die öffentliche Hand ist es notwendig, Verwaltungseinrichtungen aller Ebenen systematisch im KRITIS-Dachgesetz zu berücksichtigen. Ein einheitliches Schutzniveau ist zentral für die Stärkung der IT-Sicherheit insgesamt. Gesellschaftliche und staatliche Resilienz bedeutet auch: Es darf keine „Zwei-Klassen-Gesellschaft“ der Informationssicherheit geben. Weder im Verhältnis von Bundeskanzleramt und Bundesministerien zu den übrigen Einrichtungen der Bundesverwaltung noch im Verhältnis Staat und Privatwirtschaft. Es bedarf eines einheitlichen IT-Grundschutzes für alle Einrichtungen der Bundesverwaltung und mehr Informationsaustausch zwischen Bund und Ländern. Konsequenterweise sollte der KRITIS-Sektor „Staat und Verwaltung“ in § 4 mithin ausdrücklich aufgeführt werden. Die faktische Herausnahme eines Großteils der öffentlichen Verwaltung über die §§ 2 und 4 läuft dem Schutzzweck des Gesetzesvorhabens zuwider. In diesem Zusammenhang sollte auch der Deutsche Bundestag ausdrücklich in den Definitionsrahmen einer Kritischen Infrastruktur

aufgenommen werden, da er als Verfassungsorgan zentrale Funktionen für die staatliche Stabilität und Handlungsfähigkeit wahrnimmt.

Überdies fehlen in § 4 Abs. 1 die KRITIS-Sektoren „Forschungseinrichtungen“ sowie „Chemie“, obwohl diese mit NIS2 zumindest als wichtige bzw. besonders wichtige Einrichtungen reguliert werden. Aus Gründen der Systemkohärenz und zur Vermeidung von Schutzlücken sollten diese Bereiche auch im KRITIS-Dachgesetz Berücksichtigung finden. Entsprechendes gilt auch für den Digitalsektor: Obwohl der Begriff „Digitalsektor“ in der Gesetzesbegründung mehrfach hervorgehoben wird, findet er im eigentlichen Normtext – insbesondere in § 4 Abs. 1 – keine Entsprechung. Eine ausdrückliche Erwähnung im Gesetzestext würde die besondere Bedeutung dieses Sektors unterstreichen und zugleich zu größerer Klarheit und Rechtssicherheit in der praktischen Anwendung beitragen. Darüber hinaus ist zu berücksichtigen, dass der Entwurf den Sektor „Medien und Kultur“ nicht als eigenen KRITIS-Bereich ausweist und diesen zugleich gänzlich undefiniert lässt. Ebenso fehlen diesbezüglich konkrete Schwellenwerte oder Abgrenzungskriterien. Angesichts der zentralen Rolle freier und funktionsfähiger Medien für Informationssouveränität, Krisenkommunikation und Bevölkerungswarnung – insbesondere im Kontext hybrider Bedrohungen, Desinformationskampagnen und bewusst gesteuerter Fake-News-Strukturen – erscheint dies als gravierende Lücke. Unabhängige Medien und kulturelle Einrichtungen sind für die demokratische Willensbildung, die öffentliche Sicherheit sowie die gesamtgesellschaftliche Resilienz von herausragender Bedeutung; sie sichern Meinungsvielfalt, tragen zur Akzeptanz staatlichen Handelns bei und wirken feindlicher Einflussnahme auf öffentliche Diskurse entgegen. Kulturelle Einrichtungen leisten zudem einen wesentlichen Beitrag zur sozialen Stabilität, Identitätsbildung, Integration und Daseinsvorsorge und fungieren als Orte gesellschaftlicher Begegnung, die Polarisierung und Radikalisierung präventiv entgegenwirken können. Vor diesem Hintergrund sollte der Sektor „Kultur und Medien“ konsequent und vollumfänglich in den Schutzbereich des KRITIS-Dachgesetzes einbezogen und durch klare Definitionen sowie sektorspezifische Kriterien normativ abgesichert werden.

Besonders kritisch ist zudem § 4 Abs. 5, wonach der Zugang zu den Akten ausgeschlossen ist, die der Bestimmung kritischer Dienstleistungen zugrunde liegen. Damit fehlt den Betroffenen jede Möglichkeit, die Kriterien und Abwägungen der Einstufung nachzuvollziehen oder diese sachlich zu hinterfragen. Solange die Rechtsverordnung nach § 4 Abs. 3 nicht vorliegt, ist zudem unklar, auf welcher konkreten Grundlage die Auswahlentscheidungen beruhen. Dies führt faktisch zu einer „Blackbox-Regulierung“: Pflichten und Zuständigkeiten werden festgelegt, ohne dass überprüfbar ist, ob die zugrunde liegenden Entscheidungen sachgerecht, verhältnismäßig und mit der CER-Richtlinie konsistent sind. Zur Sicherung von Akzeptanz, Rechtssicherheit und Vertrauen bei den betroffenen Betreibern, den Aufsichtsbehörden und der Bevölkerung ist daher eine deutlich höhere Transparenz bei den Einstufungskriterien und Entscheidungsgrundlagen erforderlich – sei es durch eine präzisere gesetzliche Ausgestaltung, durch klarere Vorgaben in den Rechtsverordnungen oder durch zumindest eingeschränkte Begründungs- und Einsichtsrechte.

- **Zu § 5 KRITIS-DachG-E (Erheblichkeit einer Anlage für die Erbringung kritischer Dienstleistungen; Verordnungsermächtigung; Feststellungsbefugnis; Verordnungsermächtigung):**

  Die Betroffenheit von Betreibern ergibt sich nach dem Entwurf im Wesentlichen daraus, dass kritische Anlagen zunächst eigenständig identifiziert werden müssen. Maßgeblich ist, ob eine Anlage bestimmten Sektoren – etwa Energie, Transport und Verkehr, Finanzwesen, Sozialversicherung, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung – (§ 4 Abs. 1) zuzuordnen ist und ob definierte Schwellenwerte erreicht oder überschritten werden. Grundsätzlich ist ein Regelschwellenwert von 500.000 zu versorgenden Einwohner:innen vorgesehen. Ergänzend sollen Flexibilisierungsmöglichkeiten sicherstellen, dass auch kleinere Einrichtungen unter bestimmten Bedingungen einbezogen werden können. Wesentliche Inhalte, die die Betroffenheit bestimmen – insbesondere Anlagenarten, Schwellenwerte und Detailkategorien – werden derzeit in nachgelagerte Rechtsverordnungen ausgelagert, die noch nicht vorliegen. Aus Sicht der betroffenen Betreiber besteht jedoch ein erhebliches Bedürfnis nach frühzeitiger Rechtssicherheit. Dadurch wird eine belastbare Einschätzung der tatsächlichen Betroffenheit deutlich erschwert. Die konkretisierenden Rechtsverordnungen sollten daher zeitnah erlassen und unter angemessener Beteiligung der betroffenen Kreise ausgestaltet werden.

  In diesem Zusammenhang ist weiterhin zu konstatieren, dass die in § 5 Abs. 2 genannten Kriterien für die Bestimmung der Schwellenwerte zum Versorgungsgrad im Grundsatz sinnvoll sind, in ihrer Ausgestaltung jedoch an mehreren Stellen zu unbestimmt bleiben. Insbesondere die „*Dauer und das Ausmaß möglicher Auswirkungen* […] *auf wichtige wirtschaftliche Tätigkeiten* […] *und wichtige gesellschaftliche Funktionen*“ (Nummer 3) sowie der „*Marktanteil des Betreibers*“ (Nummer 4) werden nicht weiter konkretisiert. Ohne nachvollziehbare, sektor- und praxisgerechte Eingrenzungen – etwa durch indikative Schwellen, Beispielsfälle oder ergänzende Leitlinien – besteht die Gefahr erheblicher Rechts- und Planungsunsicherheit. Es sollte daher klargestellt werden, nach welchen Maßstäben wirtschaftliche und gesellschaftliche Auswirkungen sowie Marktanteile zu bewerten sind und wie diese Kriterien im Verhältnis zu den übrigen Faktoren zu gewichten sind.

  Überdies ist die in § 5 Abs. 3 vorgesehene Möglichkeit, dass das Bundesministerium des Innern im Einzelfall die Erheblichkeit einer Anlage für die Erbringung einer kritischen Dienstleistung feststellt – sowohl in dem Sinne, dass eine Anlage trotz Nichterfüllung der Kriterien der Rechtsverordnung als erheblich eingestuft wird, als auch in dem Sinne, dass eine Anlage trotz Erfüllung dieser Kriterien als nicht erheblich qualifiziert wird – kritisch zu beurteilen. Durch diese weitgehende Einzelfallkompetenz kann die Einstufung als kritisch oder nicht kritisch maßgeblich von einer ministeriellen Bewertung abhängen. Dies führt zu erheblicher Rechts- und Planungunsicherheit für die Betreiber, erschwert eine verlässliche und einheitliche Risiko- und Sicherheitsbewertung und birgt das Risiko zusätzlicher Belastungen durch schwer vorhersehbare Einzelentscheidungen.

Schlussendlich sollte auch der vorgesehene Regelschwellenwert von 500.000 zu versorgenden Einwohner:innen kritisch hinterfragt werden. Er ist weder transparent hergeleitet noch geeignet, die tatsächliche Kritikalität vieler Versorgungsstrukturen – etwa in der Fläche oder in Ballungsräumen mit stark vernetzten Infrastrukturen – realistisch abzubilden. **Erschwerend kommt hinzu, dass dieser Schwellenwert seit Einführung des ersten IT-Sicherheitsgesetzes unverändert verwendet wird, ohne dass seine Angemessenheit bislang einer systematischen, wissenschaftlich fundierten Überprüfung unterzogen worden wäre. Es sollte daher sektorspezifisch empirisch untersucht werden, bis zu welchen Versorgungsgrößen eine Ersatzerbringung der jeweiligen kritischen Dienstleistung noch als realistisch angesehen werden kann.** Um eine sachgerechte Abdeckung kritischer Anlagen zu gewährleisten und strukturelle Untererfassungen zu vermeiden, spricht vieles dafür, den Schwellenwert deutlich abzusenken und stärker an der konkreten Versorgungsfunktion sowie der Ausfallrelevanz auszurichten. **Die auf dieser Grundlage ermittelten Schwellenwerte sollten perspektivisch einheitlich in der BSI-Kritisverordnung, im NIS2-Umsetzungsgesetz und im KRITIS-Dachgesetz verankert werden, um eine konsistente und nachvollziehbare Abgrenzung kritischer Anlagen sicherzustellen.**

- **Zu § 7 KRITIS-DachG-E (Einrichtungen der Bundesverwaltung):**

  Grundsätzlich ist es sinnvoll, Einrichtungen der Bundesverwaltung ausdrücklich in den Anwendungsbereich des KRITIS-DachG einzubeziehen. Allerdings verstärkt die in § 7 zugrunde gelegte, sehr eng gefasste Definition der „Einrichtungen der Bundesverwaltung“ bestehende Probleme: Schon diese Einschränkung führt dazu, dass ein Teil staatlicher Strukturen aus dem Regelungsrahmen faktisch herausfällt. Hinzu kommt, dass mit dem Auswärtigen Amt und dem Bundesministerium der Verteidigung zwei besonders sicherheitsrelevante Ressorts ausdrücklich ausgenommen werden. Dies unterläuft die Kohärenz des Regelungskonzepts und sendet das Signal, dass zentrale Bundesressorts von den allgemeinen Resilienzanforderungen abgekoppelt werden können.

  Besonders kritisch ist in Absatz 2 die Konstruktion, wonach das Bundesministerium des Innern die kritischen Dienstleistungen sowie die Mindestanforderungen „im Einvernehmen“ mit den Einrichtungen der Bundesverwaltung festlegt. Durch die Möglichkeit, das Einvernehmen zu verweigern, entsteht faktisch ein Vetorecht, mit dem die tatsächlich betroffenen Bundesministerien die Umsetzung der Maßnahmen konterkarieren können. Damit wird die normative Steuerungswirkung des Gesetzes im Bereich der Bundesverwaltung erheblich geschwächt.

  Um die physische Resilienz auch in der Bundesverwaltung verbindlich zu stärken, sollte der Geltungsbereich klarer und umfassender gefasst und die Möglichkeit, Maßnahmen durch Verweigerung des Einvernehmens zu verhindern, deutlich begrenzt werden. Ausnahmen einzelner Ressorts sollten – wenn überhaupt – eng begründet und durch ergebnisäquivalente Vorgaben ersetzt werden, anstatt sie weitgehend aus dem Geltungsbereich des KRITIS-Dachgesetzes herauszunehmen. Im Ergebnis wäre es jedoch zu befürworten, die öffentliche Verwaltung vollständig in den Schutzbereich des KRITIS-Dachgesetzes aufzunehmen und Bereichsausnahmen für die Bundesverwaltung zu streichen.

- **Zu § 8 KRITIS-DachG-E (Registrierung kritischer Anlagen):**

  Die in § 8 vorgesehene Registrierungsfrist für Betreiber kritischer Anlagen bis zum 17. Juli 2026 ist vor dem Hintergrund der erheblichen Verzögerungen im Gesetzgebungsverfahren problematisch. Hierdurch verkürzt sich die tatsächlich zur Umsetzung verbleibende Zeit für die Betreiber deutlich. Um eine realistische und geordnete Umsetzung zu ermöglichen, sollte die Frist entsprechend angepasst werden, sodass die Verzögerungen im Verfahren kompensiert und ausreichende Vorbereitungs- und Umsetzungszeiträume gewährleistet werden.

  Ausdrücklich zu begrüßen ist hingegen, dass in § 8 Abs. 1 eine „gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit“ vorgesehen ist, wie es bereits in früheren Stellungnahmen angeregt worden war.

  Von besonderer Bedeutung ist zudem die Realisierung eines durchgängig digitalen Registrierungs- und Meldeportals ohne Medienbrüche. Voraussetzung hierfür ist, dass Meldungen vollständig elektronisch übermittelt werden können und anschließend eine automatisierte Weiterleitung und Bearbeitung durch die zuständigen Behörden erfolgt – ohne zusätzlichen Aufwand oder parallele Kommunikationswege für die Unternehmen.

  In diesem Zusammenhang sollte sichergestellt werden, dass bestehende Registrierungen nach dem BSIG im Sinne des angedachten Once-only-Prinzips automatisiert anerkannt und in das neue Register überführt werden, ohne dass eine erneute vollständige Registrierung erforderlich ist. Eine Übernahme der bereits vorliegenden Daten in das neue Register mit der Möglichkeit zur Ergänzung und Aktualisierung wäre sachgerecht und würde unnötige Doppelarbeit sowie zusätzliche Bürokratie vermeiden. Das hierfür vorgesehene Registrierungsportal sollte darüber hinaus Funktionen vorhalten, mit denen Unternehmen im Sinne eines Self-Service vorab selbst prüfen können, ob und in welchem Umfang sie vom Anwendungsbereich erfasst sind.

  Des Weiteren wirft § 8 Abs. 1 einzelne inhaltliche Fragen auf. Die in Nummer 4 genannten „öffentlichen IP-Adressbereiche“ sind in ihrer Zielrichtung und Reichweite nicht hinreichend transparent und bedürfen einer präziseren Konkretisierung, um Missverständnisse und überzogene Auslegungsspielräume zu vermeiden. Unklar bleibt insbesondere, ob sämtliche vom Betreiber genutzten öffentlich routbaren Netze, nur solche mit unmittelbarem Bezug zu kritischen Anlagen oder auch von Dienstleistern bereitgestellte Adressräume erfasst sein sollen und welchem konkreten Zweck diese Information dient. Zudem ist angesichts der Sensibilität dieser Daten klarzustellen, dass Erhebung und Verarbeitung nur in dem hierfür zwingend erforderlichen Umfang erfolgen. Der Begriff selbst stößt in der Praxis zudem auf Kritik, weil unklar bleibt, was genau erfasst sein soll; die nunmehr beibehaltene Formulierung birgt daher absehbar erneut Klarstellungsbedarf in der Anwendung.

- **Zu § 11 KRITIS-DachG-E (Nationale Risikoanalysen und Risikobewertungen); § 12 (Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen):**

Die in § 12 Abs. 1 verwendete Formulierung „*andere vertrauenswürdige Informationsquellen*“ ist inhaltlich zu unbestimmt und lässt offen, nach welchen Kriterien diese Vertrauenswürdigkeit zu bestimmen ist. Um die Norm klarer und praxistauglicher zu fassen, sollte klargestellt werden, dass es sich um Informationsquellen handelt, „die der Betreiber als vertrauenswürdig einstuft“ bzw. „die nach Einschätzung des Betreibers vertrauenswürdig sind“. Dies würde den notwendigen Beurteilungsspielraum der Betreiber erhalten, zugleich aber deutlicher machen, dass eine eigenverantwortliche, nachvollziehbare Auswahl zugrunde zu legen ist.

Zudem sollte klargestellt werden, dass die nach § 11 geforderten Risikoanalysen nicht zwingend auf Ebene der obersten Bundesbehörden selbst durchzuführen sind, sondern im Rahmen klar geregelter Verantwortlichkeiten auf nachgeordnete Behörden oder – unter angemessenen Qualitäts- und Kontrollvorgaben – auf externe fachkundige Stellen delegiert werden können. Dies würde der faktischen Ressourcenausstattung Rechnung tragen und zugleich ermöglichen, vorhandene Fachkompetenzen zielgerichtet zu nutzen.

Darüber hinaus sollten sich die Risikoanalysen im Schwerpunkt auf solche Gefahrenlagen konzentrieren, die im Verantwortungs- und Einflussbereich der Betreiber liegen und von diesen tatsächlich bewältigt werden können. Die vorgesehene Einbeziehung hybrider oder anderer feindlicher Bedrohungen in § 11 wirft insoweit Fragen auf, da der Schutz vor derartigen, überwiegend staatsbezogenen Gefahren primär Aufgabe staatlicher Sicherheitsbehörden ist. Vor diesem Hintergrund ist eine präzise gesetzliche Definition der in § 11 lit. c) genannten „*hybriden Bedrohungen, […] oder andere feindliche Bedrohungen*“ erforderlich, um Rechtsklarheit zu schaffen und Abgrenzungsunsicherheiten zu vermeiden.

- **Zu § 13 KRITIS-DachG-E (Resilienzpflichten der Betreiber kritischer Anlagen; Resilienzplan):**

  Betreiber kritischer Anlagen sind verpflichtet, auf Grundlage der Risikoanalysen und -bewertungen Resilienzmaßnahmen nach dem Stand der Technik zu ergreifen und dabei einen Verhältnismäßigkeitsmaßstab anzuwenden. Für die Umsetzung dieser Vorgaben steht ihnen eine Frist von 10 Monaten ab ihrer Registrierung zur Verfügung (§ 8 Abs. 7). Aus Unternehmenssicht erweist sich diese vorgesehene Frist zur Umsetzung geeigneter Resilienzmaßnahmen als nicht ausreichend. Bereits allein die Beschaffungsprozesse für erforderliche Komponenten und Systeme können diesen Zeitraum überschreiten. Eine Umsetzungsfrist von mindestens zwei Jahren würde den tatsächlichen organisatorischen und technischen Rahmenbedingungen deutlich eher Rechnung tragen.

  Überdies enthält der Entwurf des § 13 KRITIS-DachG zwar eine Auflistung entsprechender Maßnahmen, und es ist ausdrücklich zu begrüßen, dass die branchenspezifischen Resilienzstandards künftig öffentlich zugänglich beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe verfügbar sein werden, was die Transparenz erhöht und den Betreibern die Orientierung erleichtert.

  Gleichwohl ist in diesem Zusammenhang zu konstatieren, dass die in § 13 vorgesehene Aufzählung der Maßnahmen in Bezug auf die inhaltliche Ausgestaltung der

Resilienzmaßnahmen weitgehend abstrakt bleibt. Das Ziel der zugrunde liegenden EU-Richtlinie besteht ausdrücklich darin, „einheitliche Mindestverpflichtungen für kritische Einrichtungen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren“. Dem wird der Referentenentwurf jedoch nicht gerecht: Konkrete Schutz- und Vorsorgemaßnahmen werden kaum normativ festgelegt; vielmehr beschränkt sich der Entwurf im Wesentlichen darauf, Zuständigkeiten für den Erlass nachgelagerter Rechtsverordnungen zu definieren, aus denen sich die eigentlichen Betreiberpflichten erst zu einem späteren Zeitpunkt ergeben sollen. Damit wird die Umsetzung substantieller Resilienzanforderungen auf einen unbestimmten Zeitpunkt verschoben. Ob die künftig zu regelnden Mindeststandards tatsächlich geeignet sein werden, die physische Resilienz kritischer Anlagen und Systeme wirksam zu erhöhen, lässt sich auf Basis des vorliegenden Entwurfs nicht verlässlich abschätzen. Für die Betreiber entsteht dadurch ein Zustand anhaltender Unsicherheit, da weder Umfang noch Tiefe der zu erwartenden Pflichten klar erkennbar sind und somit keine belastbare Grundlage für Planung und Investitionsentscheidungen besteht.

Sinnvoll wäre es, die Resilienzpflichten systematisch entlang der etablierten Phasen des Krisenmanagements – Prävention, Vorbereitung, Bewältigung und Nachsorge – zu strukturieren. Eine solche Gliederung würde nicht nur die Verständlichkeit und Handhabung der Vorgaben erhöhen, sondern auch sicherstellen, dass Vorsorge- und Wiederanlaufmaßnahmen ebenso berücksichtigt werden wie akute Krisenreaktionen. Der vorliegende Entwurf bleibt demgegenüber in weiten Teilen additiv und unsystematisch, was die Entwicklung kohärenter Resilienzpläne durch die Betreiber erschwert.

Ferner bedürfen die in § 13 Abs. 3 vorgesehenen Pflichten hinsichtlich eines angemessenen Sicherheitsmanagements (Nr. 5) sowie verpflichtender Schulungen und Übungen (Nr. 6) einer deutlichen Konkretisierung. Die Pflicht zum Aufbau eines „angemessenen Sicherheitsmanagements“ sowie zur Durchführung verpflichtender „Schulungen und Übungen“ bleibt im Entwurf unbestimmt, obwohl die personelle Sicherheit für den Schutz kritischer Anlagen von zentraler Bedeutung ist. Erforderlich ist ein einheitlicher, überprüfbarer Wissens- und Qualifikationsrahmen für sämtliche sicherheitsrelevanten Tätigkeiten. Dies betrifft sowohl internes Personal als auch externe Dienstleister, die etwa Bewachungs-, Steuerungs-, Wartungs- oder Brandschutzaufgaben wahrnehmen. Insbesondere im Hinblick auf den Innentäterschutz sollten verbindliche Mindestanforderungen an Sicherheits- und Integritätsüberprüfungen sowie KRITIS-spezifische Kompetenzprofile normativ verankert werden. Fehlende oder heterogene Vorgaben führen andernfalls zu strukturellen Schutzlücken, die sich aufgrund des hohen Schadenspotenzials personeller Zugangsrechte unmittelbar auf die Resilienz kritischer Anlagen auswirken können. Hinzu kommt, dass viele Betreiber auf komplexe Liefer- und Dienstleistungsketten angewiesen sind, sodass unzureichend qualifiziertes oder überprüftes Fremdpersonal sektorenübergreifende Risiken erzeugt. Um ein konsistentes und belastbares Schutzniveau zu gewährleisten, sollten die personellen Anforderungen daher präzise, verbindlich und sektorenübergreifend formuliert sowie durch einheitliche Prüf- und Überprüfungsmechanismen flankiert werden.

Darüber hinaus hat sich die sicherheitspolitische Lage seit Beginn des russischen Angriffskriegs gegen die Ukraine spürbar verändert. Unbemannte Luftfahrtsysteme (Drohnen) gehören mittlerweile zum etablierten Instrumentarium staatlicher wie nichtstaatlicher Akteure. Auch in Deutschland wurden wiederholt Drohnenbewegungen im Umfeld kritischer Infrastrukturen und militärischer Liegenschaften registriert. Der vorliegende Entwurf trägt dieser Entwicklung jedoch nur unzureichend Rechnung: Konkrete Anforderungen dazu, wie Bedrohungen durch Drohnen in Risikoanalysen, Schutzkonzepten sowie in technischen und organisatorischen Resilienzmaßnahmen zu berücksichtigen sind, lassen sich aus § 13 bislang nicht entnehmen. Diese Regelungslücke ist sicherheitspolitisch problematisch, da Drohnen mit vergleichsweise geringem Mitteleinsatz erhebliche physische Schäden verursachen, Betriebsabläufe stören und Aufklärungs- bzw. Sabotagezwecken dienen können. Es sollte daher kritisch geprüft werden, ob § 13 in seiner derzeitigen Fassung den aktuellen Bedrohungslagen tatsächlich gerecht wird. Aus Sicht der Resilienz kritischer Anlagen spricht viel dafür, spezifische Vorgaben zum Umgang mit Bedrohungen durch unbemannte Luftfahrtsysteme – etwa im Rahmen der Gefährdungsanalyse, der Schutzkonzepte und technischer sowie organisatorischer Maßnahmen – ausdrücklich zu verankern.

- **Zu § 14 KRITIS-DachG-E (Sektorenübergreifende und sektorspezifische Mindestanforderungen; branchenspezifische Resilienzstandards):**

  Die in § 14 vorgesehene Möglichkeit, branchenspezifische Resilienzstandards zur Konkretisierung der Verpflichtungen nach § 13 vorzuschlagen, bildet einen zentralen Baustein des künftigen Resilienzregimes. Der Entwurf beschränkt das Initiativrecht jedoch weitgehend auf Betreiber kritischer Anlagen und ihre Branchenverbände. Damit droht eine einseitige Perspektive, die dem tatsächlichen Bedarf an fachlicher, technischer und sicherheitspraktischer Expertise nicht gerecht wird.

  Für eine tragfähige und praxistaugliche Konkretisierung sektorspezifischer Anforderungen ist es erforderlich, dass neben Betreiberorganisationen auch sachkundige Wissenschaftler:innen sowie spezialisierte Beratungs- und Dienstleistungsunternehmen systematisch in die Standardentwicklung einbezogen werden. Diese Akteure verfügen über spezifisches Know-how zu sicherheitsrelevanten Prozessen, personellen Risiken, Schutzanforderungen und Best Practices, das für die Entwicklung belastbarer Mindeststandards unerlässlich ist.

  Der Prozess der Standardbildung sollte zudem nicht als einmalige Konsultation ausgestaltet werden. Angesichts sich dynamisch entwickelnder Bedrohungslagen – insbesondere im Bereich hybrider Angriffe, technischer Innovationen und physischer Sabotageszenarien – ist ein fortlaufender, lageabhängiger und strukturierter Dialog erforderlich. Es wäre deshalb geboten, dass das BBK einen solchen Prozess vorgibt, moderiert und institutionell verankert, sodass kontinuierliches „Finetuning“ und eine adaptive Weiterentwicklung der Standards gewährleistet sind.

  Als Vorbild bietet sich die Beteiligungspraxis in der Cybersicherheit an: UP KRITIS, die Allianz für Cybersicherheit und das Cyber-Sicherheitsnetzwerk haben sich als effektive Plattformen für den fachlichen Austausch und die gemeinsame Weiterentwicklung von Standards unter

Beteiligung von Wirtschaft, Wissenschaft und Verwaltung erwiesen. Eine entsprechende Übertragung dieser kooperativen Modelle auf den Bereich der physischen Resilienz würde die Qualität, Akzeptanz und Konsistenz der branchenspezifischen Resilienzstandards erheblich stärken.

Schließlich sollte zur besseren Sichtbarkeit des Themas der physischen Sicherheit und zur Vernetzung der relevanten Akteure ein vom BMI bzw. BBK ausgerichteter „KRITIS-Sicherheitskongress" etabliert werden – vergleichbar mit dem „Deutschen IT-Sicherheitskongress" des BSI. Ein solches Format könnte als zentrale Austauschplattform dienen, auf der Betreiber, Behörden, wissenschaftliche Einrichtungen und Sicherheitsdienstleister sektorenübergreifend zusammenkommen und den Stand der Technik, neue Bedrohungsentwicklungen sowie praktische Umsetzungserfahrungen diskutieren und weiterentwickeln.

- **Zu § 16 KRITIS-DachG-E (Nachweise und behördliche Anordnungen zu Resilienzpflichten):**

  § 16 konkretisiert die Nachweisführung der Betreiber kritischer Anlagen und die Aufsichts- und Eingriffsbefugnisse der zuständigen Behörden im Hinblick auf die Resilienzpflichten nach § 13. Positiv hervorzuheben ist, dass die Norm ausdrücklich an bereits bestehende Nachweisregime anknüpft: Über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe kann die zuständige Behörde die nach § 39 BSIG beim Bundesamt für Sicherheit in der Informationstechnik eingereichten Nachweise anfordern und für die Überprüfung der Maßnahmen nach § 13 Abs. 1 heranziehen. Nach der Gesetzesbegründung soll damit sichergestellt werden, dass Nachweise zur Umsetzung von § 30 Abs. 1 BSIG zugleich als Nachweis der physischen Resilienzmaßnahmen dienen und so Doppelprüfungen und zusätzlicher Bürokratieaufwand vermieden werden.

  Gleichzeitig bleibt offen, wie die in § 16 angelegte Verzahnung zwischen BSI, BBK und den fachlich zuständigen Aufsichtsbehörden im Einzelnen organisiert und bewertet werden soll. Zwar können bereits erbrachte Nachweise in das Verfahren einbezogen werden; daneben bestehen aber eigenständige Auskunfts-, Audit- und Mängelbeseitigungsbefugnisse der nach dem KRITIS-DachG zuständigen Behörden. Ohne klar abgestimmte Bewertungsmaßstäbe und Verfahrensregelungen besteht die Gefahr, dass Betreiber trotz formell gleicher oder vergleichbarer Nachweise mit abweichenden Einschätzungen verschiedener Behörden konfrontiert werden und faktisch doch mehrfach nachsteuern müssen. Um Rechts- und Planungssicherheit zu erhöhen, wäre daher eine weitergehende Klarstellung wünschenswert, dass gleichartige oder gleichwertige Nachweise aus anderen Regimen grundsätzlich anzuerkennen sind und wie Konflikte zwischen abweichenden behördlichen Bewertungen zu behandeln sind.

- **Zu § 18 KRITIS-DachG-E (Meldungen von Vorfällen):**

  Die in § 18 vorgesehene Pflicht zur unverzüglichen Meldung von Vorfällen an die gemeinsam vom BBK und BSI eingerichtete Meldestelle ist grundsätzlich zu begrüßen, da sie eine zentrale Anlaufstelle schafft und damit zu einer besseren Gesamtsicht auf die Lage beitragen kann. Damit dieses Ziel in der Praxis erreicht wird und der Meldeaufwand für Betreiber

kritischer Anlagen beherrschbar bleibt, sind aus Sicht der Praxis jedoch einige Präzisierungen und Ergänzungen erforderlich.
Es ist zunächst positiv hervorzuheben, dass die 24-Stunden-Meldepflicht im Lichte der 1:1-Umsetzung der CER-Richtlinie und ihres Erwägungsgrundes 33 („[...] In einer solchen Meldung sollte, soweit möglich, die mutmaßliche Ursache des Sicherheitsvorfalls angegeben werden.“) praxistauglicher ausgestaltet wird.

Gleichzeitig wirft die gewählte Formulierung der Gesetzesbegründung zu § 18 Abs. 1 und 2, wonach Vorfälle bereits dann meldepflichtig sein sollen, wenn sie die Erbringung der Dienstleistung „*erheblich stören könnten“*, erhebliche Abgrenzungsfragen in der Praxis auf. Für Sachverhalte, bei denen eine Störung zwar möglich erscheint, sich aber tatsächlich nicht realisiert, stellt sich die Frage, ob eine Meldepflicht sinnvoll ist oder ob hierdurch nicht vielmehr Betreiber, Behörden und die gemeinsamen Meldestellen mit einer Vielzahl von Meldungen belastet werden, ohne dass ein entsprechender Mehrwert für die Gefahrenabwehr entsteht. Vor diesem Hintergrund erscheint es sachgerecht, die derzeitige Formulierung entweder gänzlich zu streichen oder zumindest deutlich zu schärfen. Im Falle einer Präzisierung könnte ausdrücklich an Erwägungsgrund 33 der CER-Richtlinie angeknüpft werden, wonach die Meldung so auszugestalten ist, dass „*die Ressourcen der kritischen Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden“*.

Positiv hervorzuheben ist überdies, dass das Gesetz bereits klar zwischen Erstmeldung und ausführlichem Bericht differenziert. Entscheidend wird sein, dass die vom BBK nach Absatz 3 festzulegenden Details zum Meldeverfahren und zu den Meldeinhalten so ausgestaltet werden, dass eine pragmatische Erstmeldung innerhalb von 24 Stunden mit den zu diesem Zeitpunkt verfügbaren Informationen möglich ist und Nachmeldungen bzw. Aktualisierungen bei andauernden Vorfällen nicht zu unverhältnismäßiger Bürokratie führen.

Kritisch gesehen wird, dass bestehende Meldepflichten gegenüber anderen Stellen „unberührt“ bleiben. Ohne weitere Konkretisierung droht hier ein Nebeneinander mehrerer parallel zu bedienender Meldewege. Es sollte ausdrücklich das Ziel verankert werden, dass Betreiber im Regelfall nur noch eine Meldung über die gemeinsame Meldestelle abgeben müssen und diese Meldung von dort aus automatisiert an die jeweils zuständigen Behörden und Stellen weitergeleitet wird. In diesem Zusammenhang sollte eine einheitliche Meldestelle für die Betreiber kritischer Anlagen sowie die Grundlage für einen einheitlichen, strukturierten Datenaustausch zwischen Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Bundesnetzagentur (BNetzA) und Bundeskriminalamt (BKA) geschaffen werden, sodass die zuständigen Behörden effizient und bürokratiearm zusammenarbeiten können. Zu prüfen ist daher, inwieweit bestehende Meldeverpflichtungen (z.B. gegenüber Fachaufsichten, Aufsichtsbehörden der Länder oder anderen Bundeseinrichtungen) technisch-organisatorisch in dieses zentrale Meldeportal integriert werden können.
Perspektivisch sollte ein Aufsichts- und Meldearrangement angestrebt werden, das im Sinne eines One-Stop-Shop funktioniert: Betreiber kritischer Anlagen sollten sich für Meldepflichten und wesentliche Umsetzungsfragen im Regelfall an eine zentrale Stelle

wenden können, während die Koordinierung und Weiterleitung der Informationen an BSI, BBK, sektorale Aufsichtsbehörden und Strafverfolgungsbehörden institutionell und technisch im Verantwortungsbereich des Staates liegt. Dies würde sowohl den Vollzug vereinfachen als auch die Akzeptanz der Regelungen bei den betroffenen Unternehmen erhöhen.

Für die Weiterverteilung der Informationen sind effiziente Prozesse zu definieren, die zugleich ein angemessenes Schutzniveau für sensible Informationen sicherstellen. Angesichts der Sensibilität der gemeldeten Daten sollte zudem klargestellt werden, dass für den Umgang mit diesen Informationen ein Schutzniveau gilt, das sich an den Maßstäben des Geheimschutzes orientiert. Dies betrifft insbesondere Zugriffsrechte, Speicherdauer, Zweckbindung und die Bedingungen, unter denen Informationen nach Absatz 8 an die Öffentlichkeit gegeben werden. Die Möglichkeit zur Information der Öffentlichkeit ist nachvollziehbar, darf jedoch nicht dazu führen, dass betriebskritische Details oder sicherheitsrelevante Schwachstellen offenbart werden.

Schließlich sollte § 18 stärker den Mehrwert für die meldenden Betreiber und andere potenziell betroffene Betreiber betonen. Der Entwurf sieht bislang keinen Mechanismus vor, der eine systematische Rückmeldung der Behörden an die Betreiber – etwa in Form von Lagebildern, Handlungsempfehlungen oder standardisierten Feedback-Schleifen – sicherstellt. In der derzeitigen Ausgestaltung reduziert sich der Kommunikationsfluss im Wesentlichen auf einen weitgehend einseitigen Kommunikationsprozess ohne strukturierten Rückkanal. Dies ist insbesondere deshalb problematisch, weil die Betreiber im Rahmen ihrer Verpflichtung zur Erstellung eigener Risikoanalysen auf belastbare behördliche Informationen angewiesen sind. Die in Absatz 6 vorgesehene Übermittlung „sachdienlicher Folgeinformationen“ an den betroffenen Betreiber sollte so konkretisiert werden, dass daraus ein echter Rückkanal mit praktischen Handreichungen und aktuellen Lageinformationen entsteht. Darüber hinaus sollte vorgesehen werden, dass nicht nur der unmittelbar betroffene Betreiber, sondern auch andere potenziell gefährdete Betreiber kritischer Dienstleistungen – unter Wahrung der Vertraulichkeit – gezielte Warn- und Umsetzungshinweise erhalten. Nur wenn die gemeldeten Vorfälle zu konkreten, nutzbaren Erkenntnissen für die Betreiber führen, wird sich eine hohe Meldebereitschaft und ein lebendiges, lernendes Meldesystem etablieren lassen.

- **Zu § 19 KRITIS-DachG-E (Unterstützung der Betreiber kritischer Anlagen):**

  Hervorzuheben ist, dass § 19 eine ausdrücklich unterstützende Rolle des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe vorsieht. Indem das BBK den Betreibern kritischer Anlagen Vorlagen, Muster und Leitlinien zur Umsetzung der gesetzlichen Verpflichtungen bereitstellt und ergänzend Beratungen, Schulungen und Übungen anbieten kann, wird ein praxisnaher Rahmen geschaffen, der die Umsetzung der Resilienzanforderungen erleichtert und zur Vereinheitlichung des Schutzniveaus beitragen kann.

  Darüber hinaus sollte das BBK so ausgestattet und eingebunden werden, dass es seine vorgesehene Zentralstellenfunktion tatsächlich wahrnehmen kann. Hierzu gehört, dass es

alle Informationen erhält und – wo erforderlich – selbst erheben kann, die es für die Erstellung nationaler Risikoanalysen, für die Definition einheitlicher Mindeststandards sowie für die laufende Beratung und Information der Betreiber benötigt und die Umsetzung der entsprechenden Prozesse angemessen monitoren kann.

- **Zu § 20 KRITIS-DachG-E (Umsetzungs- und Überwachungspflicht für Geschäftsleitungen):**

  Die grundsätzliche Verankerung der Verantwortung für Resilienzmaßnahmen auf Ebene der Geschäftsleitung ist zu begrüßen. Eine ordnungsgemäße Leitung eines Unternehmens bzw. einer Einrichtung umfasst längst auch die Verantwortung für physische Sicherheits- und Resilienzmaßnahmen. Insofern ist es folgerichtig, dass § 20 die Geschäftsleitungen ausdrücklich verpflichtet, die nach § 13 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung durch geeignete Organisationsstrukturen abzusichern.

  Problematisch ist jedoch, dass die Haftungsregelung in Absatz 2 sich im Wesentlichen darauf beschränkt, auf das jeweils einschlägige Gesellschaftsrecht zu verweisen: Geschäftsleitungen haften für Pflichtverletzungen nach den auf die Rechtsform anwendbaren gesellschaftsrechtlichen Vorschriften; eine eigenständige Haftung nach dem KRITIS-DachG greift nur dann, wenn solche Regelungen fehlen. In nahezu allen relevanten Rechtsformen bestehen bereits gesellschaftsrechtliche Pflichten und Haftungsregelungen für die Geschäftsleitung. Soweit § 20 lediglich auf diese bestehenden Vorschriften verweist und eine eigene Haftung nur für Fälle vorsieht, in denen überhaupt keine Regelungen existieren, entstehen faktisch keine zusätzlichen Verpflichtungen. Die Norm bleibt damit hinter dem Anspruch des Gesetzes zurück, die Resilienz kritischer Anlagen wirksam und verbindlich in der Unternehmensführung zu verankern.

  Im Gegensatz dazu verpflichtet die Umsetzung von NIS2 die Geschäftsleitungen ausdrücklich, Sicherheitsmaßnahmen zu billigen, deren Umsetzung zu überwachen und an Schulungen teilzunehmen. Um eine kohärente und wirksame Governance für physische Resilienz zu erreichen, sollte § 20 KRITIS-DachG in ähnlicher Weise konkretisiert werden. Andernfalls besteht die Gefahr, dass physische Resilienzmaßnahmen gegenüber cyberbezogenen Sicherheitsanforderungen als nachrangig wahrgenommen werden und die intendierte Steuerungswirkung des Gesetzes weitgehend verpufft. Insoweit ist auch nicht den teilweise vertretenen Auffassungen zu folgen, dass sich diese Gewährleistungsverantwortung bereits aus dem allgemeinen Gesellschaftsrecht ergäbe. Wäre dies der Fall, bedürfte es bereits keiner speziellen Regelung, da sich diese Verantwortung dann bereits aus der allgemeinen Pflicht zur ordnungsgemäßen Geschäftsleitung – etwa nach GmbHG oder AktG – ableiten ließe.

- **Zu § 22 KRITIS-DachG-E (Ausnahmebescheid):**

  § 22 sieht mit dem einfachen und erweiterten Ausnahmebescheid weitreichende Befreiungsmöglichkeiten von den Verpflichtungen des KRITIS-Dachgesetzes vor. Dies stellt eine strukturelle Schwächung des Gesetzeskonzepts dar: Anstatt für alle Betreiber kritischer Anlagen verbindliche, sektorenübergreifende Mindestpflichten festzuschreiben, wird eine

breite Öffnungsklausel geschaffen, über die zentrale Teile des Anwendungsbereichs ganz oder teilweise ausgenommen werden können. Der Anspruch des KRITIS-Dachgesetzes, einen einheitlichen Mindeststandard für physische Resilienz zu etablieren, wird damit erheblich relativiert.

Zwar ist nachvollziehbar, dass für bestimmte sicherheitssensitive Tätigkeiten besondere Regelungsregime bestehen können. In der vorliegenden Ausgestaltung droht § 22 jedoch, den zentralen Regelungsansatz des KRITIS-Dachgesetzes zu unterlaufen. Besonders problematisch ist, dass die vorgesehenen Ausnahmen gerade Einrichtungen betreffen können, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung und Strafverfolgung tätig sind oder hierfür Leistungen erbringen. Diese Bereiche sind für die staatliche Handlungs- und Funktionsfähigkeit in Krisenlagen von zentraler Bedeutung. Eine weitgehende Herausnahme dieser Betreiber führt dazu, dass ausgerechnet besonders sicherheitsrelevante Anlagen nicht denselben klaren, überprüfbaren Pflichten unterliegen wie andere kritische Einrichtungen.

Auch der Verweis darauf, die Resilienz sei „anderweitig gewährleistet und staatlich beaufsichtigt", überzeugt in dieser Allgemeinheit nicht. Er bleibt inhaltlich unbestimmt, birgt die Gefahr paralleler und unterschiedlich ausgestalteter Aufsichtsregime und steht dem Ziel eines kohärenten All-Gefahren-Ansatzes entgegen. Statt ein Nebeneinander verschiedener Sonderregelungen zu ermöglichen, sollten sämtliche Betreiber kritischer Anlagen – unabhängig davon, ob sie staatlich oder privatwirtschaftlich organisiert sind – in ein einheitliches, transparentes Regelwerk einbezogen werden. Vor diesem Hintergrund erscheint es sachgerecht, § 22 ersatzlos zu streichen. Alle kritischen Einrichtungen sollten denselben Mindestpflichten nach dem KRITIS-Dachgesetz unterliegen; nur auf dieser Grundlage lässt sich ein verlässliches, konsistentes Schutzniveau für die Versorgungssicherheit und die staatliche Krisenresilienz gewährleisten.

- **Zu § 23 KRITIS-DachG-E (Verarbeitung personenbezogener Daten):**

  Die in § 23 vorgesehenen Befugnisse zur Verarbeitung personenbezogener Daten sind im Grundsatz nachvollziehbar, bedürfen jedoch einer klareren verfassungs- und datenschutzrechtlichen Konturierung. Insbesondere sollte deutlicher hervorgehoben werden, dass personenbezogene Daten nur „soweit" erforderlich und nicht pauschal „wenn" erforderlich verarbeitet werden dürfen und dass anonymisierte oder pseudonymisierte Daten stets Vorrang haben, sofern der Zweck der Verarbeitung damit erreicht werden kann. Ferner erscheint eine präzisere Ausgestaltung der Zweckbindung angezeigt, um sicherzustellen, dass die im Rahmen des KRITIS-Dachgesetzes erhobenen Daten nicht in unbestimmter Weise für andere Zwecke genutzt werden. Dies ist nicht nur aus grundrechtlicher Perspektive, sondern auch für die Akzeptanz des Regimes bei den betroffenen Betreibern von zentraler Bedeutung.

- **Zu § 24 KRITIS-DachG-E (Bußgeldvorschriften):**

  Der in § 24 vorgesehene Bußgeldrahmen erscheint im Hinblick auf die intendierte Steuerungswirkung deutlich unterdimensioniert. Geldbußen von bis zu 500.000 Euro – in

vielen Fallgruppen sogar nur 200.000 Euro, 100.000 Euro oder weniger – stehen ersichtlich nicht in einem angemessenen Verhältnis zu den regelmäßig erforderlichen Investitionen in bauliche, technische und organisatorische Resilienzmaßnahmen. Für Betreiber größerer kritischer Anlagen besteht damit das Risiko, dass Bußgelder eher als kalkulierbare Betriebsausgabe denn als spürbare Sanktion wahrgenommen werden.

Vor diesem Hintergrund droht § 24 hinter dem Ziel eines wirksamen Vollzugs des KRITIS-Dachgesetzes zurückzubleiben. Aus Gründen der Effektivität und der Kohärenz mit der Sanktionssystematik der nationalen Umsetzung von NIS2 sollte der Bußgeldrahmen deutlich angehoben und stärker risikoadäquat bzw. unternehmensgrößenbezogen (etwa durch umsatzorientierte Obergrenzen) ausgestaltet werden.

- **Zu Artikel 5 (Inkrafttreten):**

  Nach Artikel 5 Absatz 2 sollen die Mindestvorgaben des § 14 Absatz 3 erst im Jahr 2030 in Kraft treten. Eine derart lange Übergangsfrist steht in einem deutlichen Spannungsverhältnis zur aktuellen Gefährdungslage und dem gesetzgeberischen Ziel, die Resilienz kritischer Anlagen zeitnah zu erhöhen. Über einen Zeitraum von mehreren Jahren bliebe damit ein zentrales Instrument zur Stärkung der physischen Sicherheit faktisch wirkungslos. Aus Gründen der Sicherheitsvorsorge und der staatlichen Schutzpflicht ist daher ein deutlich früheres – möglichst unmittelbares – Inkrafttreten der einschlägigen Regelungen angezeigt.

C. Fazit und weitergehender gesetzgeberischer Handlungsbedarf

Der vorliegende Entwurf des KRITIS-Dachgesetzes ist ein wichtiger, aber bislang unvollständiger Schritt hin zu einem kohärenten Schutz Kritischer Infrastrukturen. Vor dem Hintergrund der dargestellten Bedrohungslage und der unionsrechtlichen Vorgaben ist es erforderlich, über punktuelle Nachbesserungen hinaus grundlegende strukturelle Weichenstellungen vorzunehmen. Angesichts der herausragenden sicherheitspolitischen Bedeutung einer wirksamen Resilienz- und Schutzarchitektur muss der gesetzgeberische Handlungsbedarf daher klar benannt und zügig adressiert werden:

Erstens bedarf es einer **einheitlichen und integrierten KRITIS- und IT-Sicherheitsarchitektur**. Das nationale IT-Sicherheitsrecht ist bislang fragmentiert und vielfach nicht hinreichend aufeinander abgestimmt. Es sollte systematisiert und so weiterentwickelt werden, dass einheitliche IT-Sicherheitsstandards für Bund und Länder gelten und Begriffsbestimmungen mit verwandten Fachgesetzen – insbesondere dem Rechtsrahmen aus NIS2 – konsistent verwendet werden. Auf unklare und unionsrechtlich zweifelhafte Begriffe wie „vernachlässigbare Geschäftstätigkeiten“ sollte verzichtet werden. Überdies sollten Betreiber kritischer Anlagen künftig ausschließlich durch das KRITIS-Dachgesetz und die hierzu ergehenden Rechtsverordnungen bestimmt werden, um Doppelregime und Abgrenzungsstreitigkeiten zu vermeiden.

Zweitens ist die **Einbeziehung der öffentlichen Verwaltung in den Schutzbereich** konsequent fortzuführen. Die bisherige Ausklammerung weiter Teile der Bundesverwaltung sowie der Landes- und Kommunalverwaltungen führt zu systematischen Schutzlücken und einem uneinheitlichen Resilienzniveau. Bereichsausnahmen für Teile der Bundesverwaltung sollten nur in eng begründeten Ausnahmefällen und unter Sicherstellung ergebnisäquivalenter Schutzstandards beibehalten werden. Resilienzanforderungen dürfen nicht dort enden, wo staatliche Kernaufgaben beginnen. Dies gilt auch mit Blick auf den Deutschen Bundestag, der als Legislative eine zentrale Funktion für die staatliche Stabilität erfüllt und folgerichtig in den Schutzbereich einbezogen werden sollte.

Drittens ist die **institutionelle Architektur der IT-Sicherheit** weiterzuentwickeln. Das Bundesamt für Sicherheit in der Informationstechnik sollte in seiner fachlichen Unabhängigkeit gestärkt und im föderalen Gefüge zu einer echten Zentralstelle weiterentwickelt werden. Hierzu gehört auch eine verfassungsrechtliche Absicherung seiner Rolle. Die vorgesehene Funktion einer/eines Chief Information Security Officers (CISO) des Bundes sollte als hochrangige, unabhängige Stelle mit klaren Durchsetzungsbefugnissen und koordinierender Zuständigkeit für IT-Sicherheitsstandards und -aufsicht ausgestaltet werden. Ein verfassungskonformes, klar normiertes Schwachstellenmanagement ist zudem als zentraler Baustein verantwortungsvoller IT-Sicherheitspolitik rechtssicher zu implementieren.

Viertens muss der **Grundrechtsschutz, insbesondere nach Art. 10 GG,** auch im Kontext der Umsetzung von CER- und NIS2-Vorgaben gewahrt bleiben. Eingriffsbefugnisse, insbesondere zum Abruf von Bestandsdaten und zur Verarbeitung sensibler Kommunikations- und Verkehrsdaten, sind grundrechtsschonend auszugestalten. Es bedarf einer hinreichenden verfahrensmäßigen Absicherung, klarer Zweckbindungen und starker datenschutzrechtlicher

Betroffenenrechte, um sicherzustellen, dass die notwendige Stärkung der Resilienz Kritischer Infrastrukturen nicht zu einer Absenkung des Grundrechtsschutzniveaus führt.

Fünftens ist der **Mittelstand in besonderer Weise zu berücksichtigen**. Zahlreiche kleine und mittlere Unternehmen werden durch abgesenkte Schwellenwerte neu in den Anwendungsbereich einbezogen und sehen sich komplexen regulatorischen Anforderungen gegenüber. Um ihre Widerstandsfähigkeit zu erhöhen, bedarf es gezielter Beratung, unterstützender Maßnahmen und eines möglichst schlanken Vollzugs. Ein „One-Stop-Shop"-Ansatz, bei dem sich Betreiber an eine zentrale Aufsichts- oder Koordinierungsstelle wenden und diese die erforderliche Abstimmung mit anderen Behörden übernimmt, würde die Umsetzungspflichten erheblich erleichtern und Akzeptanz für die neuen Anforderungen schaffen.

Sechstens ist **Sicherheit europäisch zu denken und international zu verankern**. Deutschland kommt aufgrund seiner wirtschaftlichen Stärke und seiner politischen Rolle in Europa eine besondere Verantwortung bei der Entwicklung und Umsetzung einer kohärenten europäischen Strategie gegen hybride Bedrohungen und zum Schutz Kritischer Infrastrukturen zu. Dies umfasst eine aktive Mitgestaltung der europäischen IT-Sicherheits- und Resilienzpolitik ebenso wie die Stärkung der digitalen Souveränität, den priorisierten Einsatz vertrauenswürdiger und möglichst offener Technologien (etwa Open-Source-Lösungen in der öffentlichen Verwaltung), den Verzicht auf Anbieter mit nicht hinreichend auszuschließenden Datenabflüssen in Drittstaaten sowie eine restriktive Haltung gegenüber dem Export von Überwachungs- und Zensurtechnologie. Flankierende gesetzgeberische Maßnahmen – etwa eine Reform des sogenannten „Hackerparagraphen" um verantwortungsvolles ethisches Hacking rechtssicher zu ermöglichen, sowie eine Grundgesetzänderung zur Stärkung des BSI – sollten in diesem Zusammenhang geprüft und vorangetrieben werden.

Insgesamt zeigt sich, dass der Entwurf des KRITIS-Dachgesetzes wichtige Ansatzpunkte enthält, den gestiegenen Bedrohungen aber nur dann angemessen begegnen kann, wenn er in eine umfassende, kohärente und grundrechtskonforme Sicherheits- und IT-Strategie eingebettet wird. Ein integriertes, konsistentes und einheitliches Gesamtgefüge ist Voraussetzung dafür, die Resilienz Kritischer Infrastrukturen nachhaltig zu stärken und die Bundesrepublik Deutschland gegenüber hybriden Bedrohungen zukunftsfest aufzustellen.

Frankfurt am Main, den 27. November 2025

Prof. Dr. Dennis-Kenji Kipker
cyberintelligence.institute