AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Referentenentwurf des KRITIS-Dachgesetz vom 03.11.2025

Version 1.0 – zuletzt editiert am 27.11.2025

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen....3
2 Erforderliches Vorwort....4
3 Stellungnahme....4
§ 2 Begriffsbestimmungen; Fokus auf Anlagen....6
§ 13 Resilienzpflichten....7
Drohnendetektion, -meldung und -abwehr....7
Lagebilder....9
§ 4 Geltungsbereich; Sektoren; Verordnungsermächtigung....9
§ 5 Erheblichkeit einer Anlage für die Erbringung kritischer Dienstleistungen....10
§ 7 Einrichtungen der Bundesverwaltung....11
§ 20 Umsetzungs- und Überwachungspflicht für Geschäftsleitungen....12
§ 18 Meldewesen für Vorfälle....12
§ 22 Ausnahmebescheid....12
§ 24 Bußgeldvorschriften....13
§ 25 Evaluierung....14
Artikel 5 Inkrafttreten....14
4 Vorgehensweise....15
5 Würdigung des Prozesses....15
6 Fazit....15

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen.
Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

2 Erforderliches Vorwort

Vorab ist festzustellen, dass die vorherigen Stellungnahmen aller Verbände und auch die der AG KRITIS offenbar vollständig ignoriert wurden, was ein Unverschämtheit ist und einen **klaren Mittelfinger ins Gesicht der Zivilgesellschaft als auch der betroffenen Wirtschaft** darstellt. Das erreicht eine neue Güte von Ignoranz. Besonders in diesen Zeiten, wo hybride Gefährdungen und Sicherheitsmeldungen sich subjektiv häufen. **Realitätsferner und verantwortungsloser** kann man sich durch diese Haltung nicht aufstellen.

Wir stellen nochmals fest, dass das KritisDachG eine breite Palette relevanter Risiken adressieren soll. Dazu gehören Unfälle oder Naturereignisse – die erst durch unzureichende Resilienzmaßnahmen zu Katastrophen werden können – sowie gesundheitliche Notlagen wie Pandemien sowie hybride oder andere feindliche Bedrohungen, etwa terroristische Straftaten, kriminelle Unterwanderung oder Sabotage. Berücksichtigt werden sollen ebenso sektorübergreifende und grenzüberschreitende Risiken.

Verschiedene Einlassungen von BMI-Mitarbeitenden waren dahingehend eindeutig, dass das BMI zwischen den verschiedenen Referentenentwürfen und Anhörungen explizit nicht beabsichtigte, am Gesetzestext etwas im Sinne der verschiedenen eingereichten Stellungnahmen zu ändern. Vorhandene Wirkmechanismen nachgeordneter Behörden wurden durch das BMI unterbunden, um internen Handlungsdruck zu verhindern. Sogar Verbände von Betreibern betroffener Anlagen, die die Kosten der Umsetzung konkret tragen würden, äußerten sich uns gegenüber verständnislos für eine solch schwache Umsetzung dieser wichtigen Vorhaben.

Dieses Verhalten des BMI können wir nur als vorsätzliche Arbeitsverweigerung betrachten. **Wir sind zu der Überzeugung gekommen, dass das BMI vorsätzlich Menschenleben riskiert, um internen Abstimmungs- und Arbeitsaufwand zu reduzieren.**

3 Stellungnahme

Das KRITIS-DachG enthält auch weiterhin **kaum konkrete Festlegungen**, welche Maßnahmen nun genau ergriffen werden müssen. Das Gesetz regelt lediglich, wer welche Rechtsverordnungen erlassen muss, aus denen sich dann ergibt, was die betroffenen Unternehmen tun müssen. Auf diese Weise entzieht das Bundesministerium des Innern (BMI) nicht nur dem Parlament die Möglichkeit, konkrete Maßnahmen abzuwägen und zu besprechen. Es **verschiebt auch den Beginn echter Maßnahmen** auf einen **unbekannten Zeitpunkt in der Zukunft**, wenn nach einigen Jahren erst alle geplanten Rechtsverordnungen erlassen wurden.

Zudem ist auch ein **erheblicher Teil der Bundesverwaltung vom Gesetz ausgenommen** und die **Landesverwaltungen werden gar nicht erst adressiert** - damit sind diese Infrastrukturen im KRITIS Sektor "Staat und Verwaltung" weiterhin **physischen Risiken und hybriden Gefährdungen schutzlos ausgesetzt** und unterliegen keinen Anforderungen.

Das Ziel der EU Richtlinie lautet „einheitliche Mindestverpflichtungen für kritische Einrichtungen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren.“

Dazu stellt die AG KRITIS fest: Der vorgelegte Gesetzesentwurf enthält **keine Mindestverpflichtungen**. Stattdessen regelt der Gesetzesentwurf, welche Behörden die Verordnungen erlassen müssen, durch die sich wiederum zukünftig dann mal umzusetzende Mindestverpflichtungen ergeben würden.

Ob also die vorgesehenen Mindestverpflichtungen zum Ziel der Erhöhung der Resilienz der kritischen Anlagen und Systeme führen würden, lässt sich anhand des vorgelegten Gesetzesentwurfes nicht bewerten.

Konkrete Handlungsanweisungen für KRITIS-Betreiber sind nicht enthalten.

Der vorliegende Entwurf legt lediglich fest, welche staatlichen Strukturen die Mindestverpflichtungen zukünftig per Verordnung erlassen, prüfen und weiterentwickeln dürfen.

Das Ziel, kritische Anlagen nicht mehr nur aus der Brille der Informationstechnik (IT) zu betrachten ist richtig, da hierbei bisher nur die in diesem technischen Rahmen existenten Risiken adressiert wurden. Der hier vorgelegte “All-Gefahren-Ansatz” eignet sich besser als ein IT-zentrischer Ansatz, um die Steigerung der Versorgungssicherheit zu erreichen.

Der Gesetzentwurf **vermeidet jede klare Aussage zu Kosten und Ressourcen**. Weder für Bund und Länder noch für Betreiber lägen belastbare Zahlen vor, behauptet das BMI. Alles wird auf spätere Haushaltsverfahren verschoben. Uns sind schon vor einigen Monaten Gerüchte zugetragen worden, dass der UP KRITIS zum Erfüllungsaufwand eigene Analysen durchgeführt und bereitgestellt hat. Wenn diese Information wahr ist, ist für uns unverständlich, warum diese Zahlen hier immer noch nicht verwendet werden.

Mit der gewählten Formulierung wird die Umsetzung des KRITIS-Dachgesetzes **vollständig unter Haushaltsvorbehalt** gestellt. In der Praxis bedeutet das: Ob und wann Maßnahmen

tatsächlich umgesetzt werden, hängt von nachträglichen Finanzierungsentscheidungen der Ministerien ab. **Resilienz wird so zu einer optionalen Aufgabe**, nicht zu einer verbindlichen Pflicht. Das ist mit dem Anspruch einer systematischen und verbindlichen Stärkung kritischer Infrastrukturen unvereinbar.

§ 2 Begriffsbestimmungen; Fokus auf Anlagen

In § 2 werden die betroffenen kritischen Anlagen und kritischen Dienstleistungen definiert.

Die Begriffsbestimmung „Einrichtungen der Bundesverwaltung“ enthält nur einen **höchst lückenhaften Auszug der eigentlichen Bundesverwaltung**. Lediglich „Bundeskanzleramt, die Bundesministerien und der Beauftragte der Bundesregierung für Kultur und Medien“ werden aufgeführt.
Nicht einmal alle Bundesbehörden und Bundesministerien werden adressiert, auch alle nachgeordneten Behörden werden vollständig ausgeklammert. Laut allgemeiner Definition zählt zur Bundesverwaltung: „Behörden und Einrichtungen des Bundes, die mit dem Vollzug von Bundesangelegenheiten betraut sind.“ Nicht nur fehlen alle Behörden, die einem Bundesministerium nachgeordnet sind, also die Bundesmittelbehörden, sondern es fehlt auch die mittelbare Bundesverwaltung. Wenn wir Resilienz und Sicherheit ernst meinen, sind alle diese Behörden zu berücksichtigen.

Weiterhin bleibt unberücksichtigt, dass all jene Dienstleistungen und vor- oder ausgelagerten Produkte und Dienstleistungen, die zur Erfüllung der kritischen Dienste erforderlich sind, ebenfalls gesichert werden müssten. Diese vor- und ausgelagerten Dienste sind jedoch in der Regel sektorenunabhängig und damit vom Regelungsgehalt des KritisDachG nicht erfasst.

Ein Paradigmenwechsel - weg von der Betrachtung einzelner Anlagen und hin zu der Betrachtung der gesamten notwendigen Kette an Aufgaben oder Dienstleistungen rund um den Betrieb einer Anlage wäre sinnvoll und notwendig, um die Resilienz zu steigern.

Selbstverständlich kann man sich nicht gegen jedes Risiko wappnen, ein Restrisiko wird am Ende trotzdem überbleiben, dies sollte jedoch möglichst gering bleiben. Entsprechend sieht der Gesetzesentwurf vor, dass eine Abwägung stattfinden soll, ob eine Maßnahme gegenüber der Eintrittswahrscheinlichkeit eines Risikos verhältnismäßig ist.

Diese Abwägung wird im § 13 den Betreibenden der Anlage auferlegt.

§ 13 Resilienzpflichten

Bei dieser Abwägung der Interessen werden die Interessen der Bevölkerung (Versorgungssicherheit) sowie die Interessen des Staates (öffentliche Sicherheit) von niemandem explizit vertreten. Private Betreibende sollen folglich unter Berücksichtigung der eigenen Wirtschaftlichkeit den Risikoappetit der öffentlichen Hand festlegen.

Es wird zwar dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) das Recht gegeben, sowohl die getroffenen Maßnahmen zu prüfen, als auch Bußgelder zu verhängen, aber eine regelmäßige Auditierung - wie im BSI-Gesetz - ist nicht vorgesehen. Damit fehlen wichtige Werkzeuge, die für ein kohärentes Vorgehen unter den Betreibenden sorgen würden. Ein **Mangel an Rechtsdurchsetzung** ist daher systemisch verankert.

Die von den Betreibenden beurteilten Risiken und vorgesehenen Maßnahmen sollten daher, ähnlich wie die Prüfung nach BSI-Gesetz § 8a vorzeichnet, regelmäßig (mindestens aber alle 3 Jahre) durch unabhängige Dritte geprüft werden.

Grundsätzlich ist die **Gewinnerzielungsabsicht** für die Betreibenden der Anlagen ein **wichtigeres Ziel**, als die Sicherstellung der Resilienz und Versorgungssicherheit. Wenn ein Unternehmen sich aus freien Stücken entscheidet, eine kritische Dienstleistung für die Bevölkerung zu erbringen, so ist es angemessen, dass dieses Unternehmen die Risiken aus einem möglichen Versorgungsausfall für die Bevölkerung angemessen adressiert, auch wenn dies die Gewinne schmälert.

Drohnendetektion, -meldung und -abwehr

Seit dem Beginn von Putins Angriffskrieg auf die Ukraine hat sich die nationale Sicherheitslage deutlich verändert: Angriffe und Spionage mit Drohnen gehören inzwischen zum festen Instrumentarium staatlicher wie nichtstaatlicher Akteure. Auch in Deutschland wurden bereits viele Drohnen über kritischen Infrastrukturen und Bundeswehrliegenschaften gesichtet. Die dadurch auch als militärisches und geheimdienstliches Ziel deklarierte „Destabilisierung der Bevölkerung von Innen“ schreitet voran und verunsichert die Bevölkerung fortlaufend.

Der Entwurf enthält jedoch **keinerlei konkrete Vorgaben zur Drohnendetektion, -meldung und -abwehr**.

Diese Leerstelle ist sicherheitspolitisch problematisch, weil gerade Drohnenangriffe mit geringem Aufwand erheblichen Schaden anrichten können. Es muss deshalb kritisch hinterfragt

werden, ob § 13 **ohne klare Anforderungen an den Schutz vor unbemannten Systemen** den heutigen Bedrohungen noch gerecht wird.

Es wird daher die **Detektion, Meldung und - soweit möglich - Abwehr von Drohnen**, also unbemannten Luftfahrtsystemen, Landsystemen und Wassersystemen durch KRITIS Betreiber benötigt. Dabei ist die **Sicherheitskette (Prävention, Detektion, Alarmierung, Verifikation, Intervention, Lessons Learned)** vollständig einzuhalten und von den Betreibern konkret zu fordern.

Auch eine **Einschränkung auf Flughäfen** oder sogar lediglich auf die vier großen Flughäfen bei der Ausstattung mit einem nicht wirklich funktionalen Drohnenabwehrsystem, wie durch den Innenminister beschlossen wurde, ist wenig zielführend. Es müssen mindestens geschützt werden:

- Alle acht Kritis Sektoren aus dem BSI Gesetz,
- darüber hinaus die unregulierten Sektoren Medien & Kultur,
- sowie vor allem auch der Sektor Staat & Verwaltung,
- als auch der Sektor Großforschungseinrichtungen & und der Sektor Chemie.
  (Die beiden letztgenannten sind stand heute leider immer noch nicht als KRITIS definiert worden)
- Darüber hinaus benötigen auch militärische Einrichtungen Regelungen dieser Art, aber diese können nicht in diesem Gesetz festgelegt werden.

Generell stehen auch Störfallbetriebe und kritische Industrie dem Thema schutzlos gegenüber.

Drohnen werden beispielsweise auch von Ingenieuren durch Automatisierung als Roboter eingesetzt. Exemplarisch genannt sei hier bei der Begutachtung von möglichen Schäden an Brückenanlagen. Das Einsatzszenario als programmierter Roboter, der vorkonfigurierte Strecken und Befehlsketten tätigt, muss wahrgenommen und adressiert werden.

Bedrohungsoptionen durch Drohnen sind insbesondere:

- Angriffe auf Menschenmengen,
- Drohnen, die mit Explosivstoffen, chemischen oder biologischen Stoffen ausgerüstet sind
- Angriffe auf kritische Infrastruktur wie LNG-Terminals oder Energieanlagen,
- koordinierte Mehrfachangriffe
- Spionage

Drohnen können aber auch Gegenstände tragen oder abwerfen. Möglich sind hierbei Abhöranlagen, Störsender, WLAN-Router, Sprengkörper zu Luft und Wasser oder auch ein Raspberry Pi mit Akkupack und vieles mehr.

Bilder und Videos von Drohnen können im Nachgang (teil-)automatisiert oder sogar KI unterstützt ausgewertet werden. Auch durch Einsatz von Gesichtserkennung und biometrische Analysen.

Optionen, die uns noch bevorstehen, sind „Schwarmintelligenz“ (als Ausdruck für den koordinierten Einsatz mehrerer Drohnen) oder Drohnen mit Kamikaze-Funktionalität.

Es gibt leider **keine Silver-Bullet Lösung bei der Abwehr von Drohnen**. Das hindert uns aber nicht daran, bereits vorhandene mögliche und gute Maßnahmen in der Breite der KRITIS Betreiber zu etablieren und in der Forschung aufgrund solcher gesetzlicher Forderungen den Stand der Technik zur Abwehr - auch und insbesondere in Friedenszeiten – weiterzuentwickeln. Und insbesondere hindert es uns auch nicht daran, eine vollständige Umsetzung von Drohnendetektion und Drohnenmeldungen vorzunehmen, die dann in ein entsprechendes Lagebild fließen können.

Lagebilder

Hilfreich zur Transparenz und Aufklärung als auch zur Abwehr von Desinformation ist auch im Zusammenhang mit z.B. der bereits oben erwähnten Drohnenabwehr, wenn alle Lagebilder immer - zusätzlich zu den geheimen Versionen - öffentlich verfügbar sind.

Sinnvollerweise sollten diese Daten direkt als maschinenlesbare Datensätze über offene Standard und Schnittstellen bereitgestellt werden. Ein positiv hervorzuhebendes Beispiel dazu ist das European Repository of Cyber Incidents (EuRepoC)[1] für Cyberangriffe, das als Vorbild für die Sammlung und Bereitstellung von Drohnenmeldungen dienen kann.

§ 4 Geltungsbereich; Sektoren; Verordnungsermächtigung

Der KRITIS Sektor Staat und Verwaltung ist auch in diesem Entwurf weiterhin unzureichend adressiert. Aus § 4 ist “Staat und Verwaltung” komplett gestrichen worden, aber darüber hinaus sind auch Kommunalverwaltungen und Behörden der Länder unzureichend geregelt.

1 https://eurepoc.eu/de/home-deutsch/

Da auch durch diese Behörden Dienstleistungen erbracht werden, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können, halten wir eine Regelung der physischen Sicherheit dieser Anlagen auch in diesem Bereich für unumgänglich.

Konsequenterweise sollte in § 4 ebenso der KRITIS Sektor „Staat und Verwaltung“ aufgeführt werden. Um eine Überregulierung, dort wo diese zu befürchten ist, zu vermeiden, kann die Bundesverwaltung von den Regelungen in § 5 (3) Gebrauch machen. Eine pauschale Ausklammerung des Großteils der Bundesverwaltung über die Definition in § 2 und § 4 konterkariert die Zielerfüllung des Gesetzesvorhabens.

In § 4 vermisst die AG KRITIS außerdem den KRITIS Sektor Chemie und Großforschungseinrichtungen, analog zum NIS2UmsuCG, wo diese wenigstens als besonders wichtige oder wichtige Einrichtungen reguliert werden.

§ 4 (5) schließt den Zugang zu den Akten aus, die die Bestimmung kritischer Dienstleistungen betreffen. Damit fehlt jede Möglichkeit, die Kriterien und Abwägungen der Einstufung nachzuvollziehen. Solange die Rechtsverordnung nach § 4 (3) nicht vorliegt, ist nicht klar, auf welcher Grundlage diese Auswahl erfolgt. Die Folge ist eine Blackbox-Regulierung: Pflichten und Zuständigkeiten werden festgelegt, ohne dass überprüfbar wäre, ob die getroffenen Entscheidungen sachgerecht, verhältnismäßig und konsistent mit der EU CER-Richtlinie sind. Transparenz ist jedoch zwingende Voraussetzung, um Akzeptanz und Rechtssicherheit für die betroffenen Betreibenden wie auch für die Aufsichtsbehörden und zuletzt auch für die Bevölkerung zu gewährleisten.

§ 5 Erheblichkeit einer Anlage für die Erbringung kritischer Dienstleistungen

Hier finden sich einige **minimale Regelungsansätze**, die allerdings ausschließlich Bundesministerien und das Bundeskanzleramt betreffen, dann allerdings weitere Ausnahmen für eine ganze Reihe von Tätigkeitsbereichen vorsehen.

Den Ministerien unterstellte, nachgeordnete Behörden, wie zum Beispiel die BDBOS, sollten miterfasst werden.

Landes- und Kommunalverwaltungen sind von den Regelungen nicht betroffen. Es wäre **dringend notwendig**, den KRITIS Sektor Staat und Verwaltung – sowohl durch Erlass einer entsprechenden KRITIS-Verordnung, als auch im KRITIS-Dachgesetz gleichwertig zu betrachten und zu regeln.

Landes- und Kommunalverwaltungen sind oftmals nicht ausreichend ausgestattet, um die notwendige 24/7 Überwachung und Administration der IT-Systeme und der physischen Sicherheit zu gewährleisten. Hieraus entsteht ein **politischer Handlungsbedarf des Bundes**, Ressourcen übergreifend zu organisieren und Synergien zu schaffen. Die zahlreichen (Cyber-)angriffe auf die öffentliche Hand dokumentieren ein **flächendeckendes, mangelhaftes Sicherheitsniveau**, welches aus unserer Sicht ausreicht, um den Handlungsbedarf zu rechtfertigen.

§ 5 (2) letzter Satz: „Der Regelwert für Schwellenwerte beträgt grundsätzlich 500 000 von einer Anlage zu versorgende Einwohner."

Dieser Schwellwert wird seit 2016, als das erste IT-Sicherheitsgesetz erlassen wurde, verwendet. Bis heute wurde dieser **Schwellwert nicht wissenschaftlich untersucht**, sondern aufgrund der Versorgungsmöglichkeit der Rettungskräfte mit dieser Menge Menschen an Ersatzstrom in einem Katastrophenwinter vor vielen Jahren ungeprüft übernommen. Wir fordern die **Durchführung einer wissenschaftlichen Untersuchung**, bis zu welchem Schwellwert eine Ersatzerbringung der kritischen Dienstleistung jeweils pro Sektor oder Anlage für möglich erachtet wird. Diese wissenschaftlichen Schwellwerte sollen daraufhin die Schwellwerte in der BSI-Kritisverordnung, im NIS2UmsuCG und im KRITIS-DachG harmonisiert und einheitlich ersetzen.

Der Bundesrat stellt in seiner Stellungnahme zum KritisdachG - Drucksache 558/25[2] vom 21.11.2025 klar heraus:
„Was zur Kritischen Infrastruktur in Deutschland gehört, muss umfassend, abschließend und bundesweit definiert werden, um in der Praxis einen einheitlichen Vollzug der Maßnahmen in Bund, Ländern und Kommunen sowie auf Betreiberseite rund um den Schutz und die Resilienz der Kritischen Infrastruktur sicherzustellen." und legt nachfolgend dar, dass **erheblicher Defizite in entsprechenden KatSchutz-Kapazitäten für alle KRITIS-Bereiche** bestünden, so dass **überhaupt keine Notversorgungsmöglichkeiten (des KatS)** vorhanden sind, und „folglich müsste der **KRITIS-Schwellenwert hier bei null** liegen".

Der Stellungnahme des Bundesrat stimmen wir vollständig zu.

§ 7 Einrichtungen der Bundesverwaltung

In Absatz 2 stimmt das BMI die kritischen Dienstleistungen und die Mindestanforderungen im Einvernehmen mit den besonders restriktiv definierten „Einrichtungen der Bundesverwaltung"

2 https://www.bundesrat.de/SharedDocs/drucksachen/2025/0501-0600/558-25(B).pdf?__blob=publicationFile&v=1

ab. Durch die **Verweigerung des Einvernehmens** können also alle Bundesministerien, die tatsächlich betroffen sind, die **Umsetzung der Maßnahmen konterkarieren**. Auch wenn die unüblich enge Definition der „Einrichtungen der Bundesverwaltung“ schon an sich kritikwürdig ist, **werden hier weitere Ausnahmen geschaffen**, denn das „Auswärtige Amt und das Bundesministerium der Verteidigung“ werden hier noch zusätzlich vom Geltungsbereich ausgeklammert.

§ 20 Umsetzungs- und Überwachungspflicht für Geschäftsleitungen

§ 20 KRITIS-DachG darf nicht hinter den Vorgaben des NIS2UmsuCG zurückbleiben. Der Entwurf verweist lediglich auf das bestehende Gesellschaftsrecht: „Geschäftsleitungen, die ihre Pflicht […] verletzen, haften ihrer Einrichtung […] nach den auf die Rechtsform […] anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn […] keine Haftungsregelung enthalten [ist].“

Das bedeutet: Wenn es in der jeweiligen Rechtsform ohnehin Regeln zur Haftung gibt – was bei fast allen Unternehmen der Fall ist – **fügt das Dachgesetz nichts hinzu**. Nur wenn gar keine Vorschrift existiert, würde eine Ersatzhaftung greifen.

Damit entstehen **für Geschäftsleitungen faktisch keine neuen Verpflichtungen**. Im Gegensatz dazu verpflichtet das NIS2UmsuCG die Geschäftsleitungen ausdrücklich, Sicherheitsmaßnahmen zu billigen, deren Umsetzung zu überwachen und an Schulungen teilzunehmen; Verstöße sind zudem bußgeldbewehrt mit Beträgen bis zu 10 Mio. € oder 2 % des Jahresumsatzes.

Es ist zwingend erforderlich, dass § 20 KRITIS-DachG dieselbe Verbindlichkeit schafft. Die Haftung der Geschäftsleitungen für physische Resilienzmaßnahmen muss klar, persönlich und mit spürbaren Sanktionen geregelt werden – gleichlaufend zum NIS2UmsuCG und nicht abgeschwächt.

§ 18 Meldewesen für Vorfälle

Der Entwurf des KRITIS-DachG verpflichtet BBK und BSI, eine gemeinsame Meldestelle für Vorfälle einzurichten (§ 12). Dies halten wir für **den richtigen Weg**, um im Falle eines Vorfalles den Aufwand für Unternehmen zu reduzieren.

§ 22 Ausnahmebescheid

§ 22 Ausnahmebescheid stellt eine **systematische Schwächung des Gesetzes** dar. Statt einheitliche Mindestpflichten für alle Betreiber kritischer Anlagen verbindlich festzulegen, eröffnet die Regelung eine weitreichende Öffnungsklausel. Damit wird der zentrale Anspruch des KRITIS-Dachgesetzes – die Herstellung eines sektorenübergreifenden Mindeststandards – ausgehebelt.

Die vorgeschlagenen **Befreiungen für Betreibende mit Bezug zu nationaler Sicherheit, öffentlicher Sicherheit, Verteidigung oder Strafverfolgung** sind nicht sachgerecht. Gerade diese Bereiche sind für das Funktionieren des Staates im Krisenfall essenziell. Eine Herausnahme führt dazu, dass ausgerechnet die **sicherheitskritischsten Anlagen ohne einheitliche, überprüfbare Pflichten** bleiben.

Auch die Konstruktion einer „anderweitig gewährleisteten und staatlich beaufsichtigten“ Resilienz überzeugt nicht. Sie schafft **unklare Doppelstrukturen und widerspricht dem Ziel** eines kohärenten All-Gefahren-Ansatzes. Statt ein **Flickwerk verschiedener Aufsichtsregime** zuzulassen, müssen alle Betreibende, ob staatlich oder privatwirtschaftlich, in ein gemeinsames Regelwerk eingebunden sein.

Wir fordern, **§ 22 vollständig zu streichen**. Alle kritischen Einrichtungen müssen denselben Mindestpflichten nach diesem Gesetz unterliegen – **ohne Ausnahmen**. Nur so lässt sich Versorgungssicherheit verlässlich gewährleisten.

§ 24 Bußgeldvorschriften

Die im Entwurf **vorgesehenen Bußgelder sind nicht geeignet**, die Einhaltung der Pflichten durchzusetzen. Mit maximal 500.000 € - in vielen Fällen sogar nur 200.000 € oder weniger - bleiben die Summen weit hinter den tatsächlichen Kosten zurück, die für übliche bauliche, technische und organisatorische Resilienzmaßnahmen aufzubringen sind.

Der Aufbau und Betrieb eines ernsthaften Resilienz- oder Schutzkonzepts (z. B. bauliche Sicherungen, Notstromversorgung, Redundanzen, Personaltraining) kostet ein Vielfaches dieser Beträge. **In der Praxis entsteht damit ein falscher Anreiz**: Es ist für Unternehmen günstiger, die Pflichten zu ignorieren und im Zweifel ein Bußgeld zu zahlen, als die notwendigen Investitionen in Resilienz zu tätigen.

Für Betreiber kritischer Anlagen wird es damit ökonomisch sinnvoller, Bußgelder zu kalkulieren, statt in die geforderten Schutzmaßnahmen zu investieren.

Im direkten Vergleich zeigt sich, dass das NIS2UmsuCG wesentlich schärfere Sanktionen vorsieht: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes. Dort sind die Beträge so bemessen, dass sie auch bei großen Unternehmen eine echte Wirkung entfalten. Der vorliegende Entwurf bleibt dagegen **ein zahnloser Tiger**. Ohne eine deutliche Anhebung der Bußgeldrahmen **verliert § 24 jede Steuerungswirkung** und gefährdet die Umsetzung der gesetzlichen Ziele. Eine Angleichung an die Bußgeldmechanismen des NIS2UmsuCG ist zwingend erforderlich.

§ 25 Evaluierung

Obwohl die grundsätzliche Idee hier richtig ist, fehlt hier, dass dieser Evaluierungsbericht zur Transparenz regelmäßig und durch Dritte einsehbar veröffentlicht wird. Auch fehlt die Festlegung in welchem Zeitrahmen das KritisDachG „regelmäßig“ evaluiert wird. Wir halten die **Frist für die erstmalige Evaluierung durch das BMI für zu lang** und empfehlen dem BMI, die Dringlichkeitsargumentation aus dem Einladungsschreiben zu der Verbändeanhörung auch hier anzuwenden und die Evaluierung entsprechend früher durchzuführen. Auch weitere Berichtspflichten würden wir begrüßen - z.B. ein **regelmäßiger Bericht an den Deutschen Bundestag**.

Artikel 5 Inkrafttreten

Absatz 2: Die Mindestvorgaben nach § 14 (3) sollen **erst in 2030 in Kraft treten**. Aus unserer Sicht ist diese **Wartezeit staatsgefährdend und grob fahrlässig**. Wir fordern das sofortige Inkrafttreten aller Vorschriften des KRITIS-Dachgesetzes ohne weitere Verzögerungen.

4 Vorgehensweise

Das BMI hat seine gesetzliche Pflicht erfüllt, die Wirtschaft anzuhören. Neben den Anhörungen gab es darüber hinaus auch ein Werkstattgespräch – zu welchem das BMI nicht verpflichtet war. Wir sind dem BMI dankbar, explizit zu beidem eingeladen worden zu sein und darüber hinaus auch zu bestimmten Entwurfsstadien um schriftliche Stellungnahmen gebeten worden zu sein.

Wir möchten besonders hervorheben, dass wir manche Referentenentwürfe zu diesem Gesetz im Änderungsmodus bekommen haben. Der Änderungsmodus erlaubt, direkt klar sehen zu können, welche Wörter im Vergleich zur Vorversion geändert, gelöscht oder ergänzt wurden.

Noch beim IT-SiG2 haben wir uns sehr deutlich und laut darüber beschwert, dass die in schneller Folge veröffentlichten Entwurfsversionen nur den Text enthielten, aber keine Informationen über Änderungen. Für dieses Gesetz hat sich der Prozess aus unserer Sicht an dieser Stelle deutlich verbessert.

5 Würdigung des Prozesses

Abschließend betonen wir als AG KRITIS erneut, dass ein transparenter Prozess in der Gesetzgebung sowie umfassende und zeitlich angemessene Beteiligungsverfahren der Wirtschaft, Wissenschaft und Zivilgesellschaft bei derart tiefgreifenden und weitreichenden Gesetzgebungsverfahren dringend geboten ist und bei diesem Vorhaben **weitestgehend berücksichtigt** wurde.

Insbesondere hinsichtlich einer einheitlichen und kongruenten Regulierung im KRITIS-Umfeld betrachten wir als AG KRITIS eine gleichzeitige Veröffentlichung und Diskussion von Gesetzesentwürfen zur Umsetzung der EU NIS2-Richtlinie (NIS2UmsuCG) und EU CER-Richtlinie (KRITIS-Dachgesetz) sowie der im NIS2UmsuCG vorgesehenen Verordnungen für **zwingend erforderlich**.

6 Fazit

Es bleibt festzuhalten, dass **weiterhin keine vollständige Harmonisierung** der Regelungen zwischen den beiden Gesetzesvorlagen NIS2-Richtlinie (NIS2UmsuCG) und CER-Richtlinie (KRITIS-Dachgesetz) erfolgt ist. Eine hinreichende Überprüfung ist aktuell aufgrund mangelnder Transparenz nicht leistbar. **Übrig bleibt eine unsichere Lage** bei allen potenziell betroffenen Einrichtungen und ihren Lieferketten, sowie bei allen verantwortlichen

Aufsichtsbehörden und Zuständigen für die Umsetzung und Einhaltung der kommenden Regulierungen als auch bei der Wissenschaft, Forschung und zuletzt auch der fachkundigen Bevölkerung, die willens sind, ihren Beitrag durch Fachexpertise ehrenamtlich und kostenfrei beizutragen, dies aber nicht angemessen in den intransparenten Dialog einbringen können.

Das Wimmelbild der Verantwortungsdiffusion wird also weiterhin gefestigt und bleibt stabil & beständig. Deutschland bleibt unnötig ungesichert.

Die NIS2-Richtlinie soll in erster Linie eine defensive Cybersicherheitstrategie sein, welche bisherige Strukturen stärkt und EU-weit harmonisiert, so wie die EU CER-Richtlinie dies für physischer Sicherheit abdecken soll. Dies geht nur, wenn beides harmonisiert Berücksichtigung findet.

Für Deutschland würde sich hier die einmalige Chance bieten, die gewachsenen Verantwortlichkeiten, die mit dem "Wimmelbild der Verantwortungsdiffusion" in der Öffentlichkeit bekannt sind, aufzuräumen. Konkret bedeutet das, alle Ebenen im Staat gemeinsam in die Lage zu versetzen, effektiv Cyber- und physische Sicherheit herzustellen. In der Wirtschaft werden längst höhere Maßstäbe angesetzt, die staatliche Einrichtungen und öffentliche Verwaltungen nicht leisten müssen. Wenn aus Deutschland eine (auch physisch resiliente) Cybernation werden soll, dann muss die Regierung aufhören hier Ausnahmen zu machen, sondern hart arbeiten, anpacken und kompromisslos umsetzen.

Physische- und Cybersicherheit sind eine gesamtgesellschaftliche Leistung und an der Spitze muss ein moderner Staat als Vorbild stehen. Ein Staat der versteht, das offensive Optionen im Cyber- und Informationsraum vor allem seinen BürgerInnen schadet. Die kürzlich geäußerten Forderungen nach einem "Cyberdome" zeigen, dass auch der neue Bundesminister des Inneren nicht verstanden hat, wie der Cyberraum funktioniert.

Jeder IT-Sicherheitsforscher wird bestätigen, dass wir im Cyberraum hohe Burgmauern und tiefe Burggräben benötigen, aber keine Kanonen und erst Recht keinen Cyberdome.

Statt Milliarden für KI-Gigafactorys auszugeben wäre es dringend notwendig, die Brot-und-Butter Aufgaben der physischen Sicherheit und einer resilienten Digitalisierung auskömmlich zu finanzieren und konsequent umzusetzen. Damit kann man zwar keine Schlagzeilen machen, aber – und nur das sollte zählen – die Bevölkerung vor physischen und Cyberangriffen und deren Auswirkungen schützen.

Statt viel Geld in bürgerrechtsverachtende Spionagesoftware aus dem Hause Palantir zu investieren wäre es zielführender, ein durchgängig hohes physisches und IT-Sicherheits- und Resilienzniveau auf allen Ebenen des Staates umzusetzen und den Ländern bei der Einführung von Software ohne verfassungsrechtliche Defizite zu helfen.

Manuel ‚HonkHase' Atug, Gründer und Sprecher der unabhängigen AG KRITIS zum aktuellsten Entwurf:

„Seit dem letzten Entwurf und den Stellungnahmen dazu sind genau zwei Tippfehler und eine Referenz geändert worden. Das ist ein **Mittelfinger in das Gesicht der Zivilgesellschaft und der Wirtschaft zugleich** und erreicht damit einen **neuen Höhepunkt an Dreistigkeit**. Die Verantwortlichen für die Sicherheit in Deutschland scheinen **mit Vorsatz keine Handlungen** aus den hybriden Gefährdungen der letzten Monate ableiten zu wollen. Ab wann werden solche Menschen eigentlich als Gefährder eingestuft?

Alle(!) Defizite aus vorherigen Entwürfen bleiben daher weiterhin vollständig bestehen, so dass die Forderungen der AG KRITIS, sie abzustellen, ebenfalls vollständig aufrechterhalten werden. Die EU hat Vorgaben zu defensiver physischer und Cyberresilienz aufgestellt, aber **Deutschland bleibt mit dem aktuellen Kritis-Dachgesetz Gesetzesentwurf weiterhin peinlich weit hinter diesem Ziel zurück.**

Lobend hervorzuheben ist immerhin immer noch, dass die branchenspezifischen Resilienzstandards öffentlich beim BBK abrufbar sein werden."