21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)102 H
vom 1. Dezember 2025

Schriftliche Stellungnahme

von Dr. Jürgen Harrer, Universität der Bundeswehr München, Center for Intelligence and Security Studies vom 30. November 2025

Öffentliche Anhörung

zu dem

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/2510

Stellungnahme
als Sachverständiger

zum

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen
BT-Drucksache 21/2510

Vorbemerkung

Deutschland braucht rasch ein gutes KRITIS-Dachgesetz.

Neben den bereits vorhandenen Mindeststandards im Bereich der digitalen Sicherheit, werden nun endlich auch Mindeststandards für den Bereich der physischen Sicherheit Kritischer Infrastrukturen formuliert.

Der vorliegende Gesetzentwurf ist mit den gesetzten Schwerpunkten grundsätzlich auf dem richtigen Weg und kann dazu beitragen, die Resilienz der KRITIS-Betriebe und damit auch die Resilienz der Wertschöpfungs- und Lieferketten der deutschen Wirtschaft zu stärken.

Überblick - die in dieser Stellungnahme adressierten Themen

1 Erfüllungsaufwände und weitere Kosten 2
2 Individuelle Resilienz und kollektive Resilienz 3
3 Orientierungswert statt Regelschwellenwert 3
4 Implementierung in zwei Wellen 4
5 Grenzen klassischer Sicherheitskonzepte - wenn Schutz nicht gelingt 5
6 Resilienz vs. Effizienz 6
7 Konvergenz physischer und digitaler Sicherheit 6

1 Erfüllungsaufwände und weitere Kosten

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger (S. 4)

„Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger."

Diese Einschätzung dürfte nicht zutreffen.

Die neuen Resilienzanforderungen u.a. im Bereich der Standortsicherheit (Sicherheitszaun, Zutrittssteuerung, Sensoren, Videotechnik etc.) werden bei vielen betroffenen KRITIS-Betreibern zu hohen Investitionen in den Auf- und Umbau von Infrastruktur sowie zu hohen Betriebskosten für personelle und organisatorische Sicherheitsmaßnahmen führen.
Es ist zu erwarten, dass sowohl die einmaligen, als auch die laufenden Kosten auf die erbachten Leistungen umgelegt und an die Bürgerinnen und Bürger weiterverrechnet werden.

Insofern wäre die bei „E.2 Erfüllungsaufwand für die Wirtschaft" (S. 4) gewählte Formulierung hier sinngemäß zu verwenden: „Für Bürgerinnen und Bürger entsteht ein Erfüllungsaufwand, der in seiner Gesamtheit zum jetzigen Zeitpunkt noch nicht geschätzt werden kann".

E.2 Erfüllungsaufwand für die Wirtschaft (S. 4-5)

Wie in den o.a. Ausführungen zu E.1 dargestellt, werden vielen Betreibern kritischer Anlagen für die Umsetzung der geforderten Resilienzmaßnahmen hohe einmalige und hohe laufende Kosten entstehen.

Um gerade bedürftige kleinere und mittlere Betriebe nicht zu überlasten, wäre es sinnvoll, wenn diesen Unternehmen eine finanzielle Unterstützung mit zwei Ansatzpunkten gewährt würde:

Einerseits könnten ihnen vergünstigte Kredite die erforderliche Liquidität für die zu erwartenden Umbau- und Aufrüstmaßnahmen ermöglichen. Andererseits könnten ihnen angemessene Sonderabschreibungen helfen, die Steuerlast in den ersten investitionsintensiven Jahren zu mindern.

F Weitere Kosten (S. 5)

„Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und das Verbraucherpreisniveau sind nicht zu erwarten."

Diese Einschätzung dürfte nicht zutreffen.

Wie in den o.a. Ausführungen zu E.1 dargestellt, sind durchaus konkrete Auswirkungen auf Einzelpreise, das allgemeine Preisniveau und das Verbraucherpreisniveau zu erwarten.

2 Individuelle Resilienz und kollektive Resilienz

Im Gesetzentwurf sind vor allem individuelle Resilienzmaßnahmen dargestellt, die dazu führen sollen, dass jedes regulierte Unternehmen bei sich im eigenen Haus ein angemessenes Mindestmaß an Selbstschutz gegenüber physischen Bedrohungen etabliert.

Für das Funktionieren des Systems von KRITIS-Organisationen (privat und staatlich) wird es zudem darauf ankommen, die kollektive Resilienz aller Beteiligten und ihrer wechselseitigen Abhängigkeiten zu stärken.

Sinnvoll wäre hier u.a. eine überregionale Steuerungsfunktion, die nicht nur Meldungen entgegennimmt und die Implementierung des KRITIS-Dachgesetzes überwacht, sondern auch sicherheitsbezogene Informationen an betroffene und möglicherweise bedrohte KRITIS-Organisationen weitergibt.

Wenn es ein entsprechendes Lagebild z.B. ermöglichen würde zu erkennen, dass gleichzeitige Ereignisse in Bremen, Hamburg und Hannover Teil eines mehrphasigen (hybriden) Angriffs sind und demnächst ähnliche Ereignisse in Berlin, Leipzig und Dresden zu erwarten sind, dann könnte die kollektive Resilienz dadurch enorm gesteigert werden.

Hilfreich wäre hierbei auch eine „Plattform zur Bedrohungsfrüherkennung“, die u.a. einen wechselseitigen, bidirektionalen Austausch relevanter Informationen zwischen Behörden und Unternehmen unterstützt (vgl. die „Eckpunkte der Nationalen Wirtschaftsschutzstrategie“ des BMI vom Februar 2024).

Auch die Fähigkeit, ein „Interdisziplinäres Lagebild in Echtzeit“ zu erzeugen, das durch entsprechende Lageprodukte die Lageführung bei Parallel-Ereignissen und überregionalen Ereignissen unterstützt, würde die kollektive Resilienz der handelnden Akteure deutlich stärken. Dies wäre wichtig insbesondere bei Großschadenslagen und bei mehrphasigen (hybriden) Angriffen, die zeitgleich an verschiedenen Orten des Landes stattfinden. (vgl. Grünbuch „Interdisziplinäres Lagebild in Echtzeit“ des ZOES e. V. vom März 2023).

3 Orientierungswert statt Regelschwellenwert

Eine echte Resilienz der Gefahrengemeinschaft von Staat, Wirtschaft und Bürgern kann nur dann zu erreichen sein, wenn sich alle Akteure in angemessener Weise daran beteiligen.

Der Regelschwellenwert von 500.000 (von einer Anlage zu versorgenden Einwohnern) sendet womöglich die Botschaft: Die großen Betreiber müssen sich schützen und alle anderen nicht.

Das wäre ein fatales Signal!

Tatsächlich findet sich im §5 noch eine Reihe weiterer Kriterien zur Ermittlung von Kritikalität und zur Klassifizierung Kritischer Infrastrukturen.

In den Erläuterungen zu §5 Absatz 2 finden sich auf S. 56 folgende Ausführungen:

„Die Kriterien sind soweit es geht kumulativ für die Erarbeitung der Schwellenwerte zu berücksichtigen. Es können sich bei der Bewertung der Kritikalität der jeweiligen

Anlagenkategorie unterschiedliche Gewichtungen bezüglich der Kriterien ergeben. (...) Abweichungen von diesem Regelschwellenwert können dabei im Einzelfall sinnvoll sein.“

„Insbesondere können auch unter Zuhilfenahme qualitativer Kriterien (Beispiel: einzige versorgungsrelevante Anlage in einem größeren Umkreis oder aufgrund ihrer technischen Eigenschaften besonders relevante Anlage) bei einzelnen Anlagenkategorien mehrere unterschiedliche quantitative Kriterien festgelegt werden, um eine möglichst sachgerechte Bestimmung kritischer Anlagen sicherzustellen.“

Um Missverständnisse zu vermeiden wäre es daher sinnvoll, den Begriff „Regelschwellenwert“ durch den Begriff „Orientierungswert“ zu ersetzen - wenn bei der angestrebten „sachgerechten Bestimmung“ eine Einzelfallbetrachtung unter Berücksichtigung mehrerer unterschiedlich gewichteter Kriterien vorgesehen ist.

4 Implementierung in zwei Wellen

Seit etwa einem Jahr wird in der deutschen Security Community auch diskutiert, wie die Implementierung des KRITIS-Dachgesetzes vermutlich verlaufen wird. Erwartet werden zwei Wellen bei der Umsetzung:

1.Welle:

Eine niedrige vierstellige Anzahl von Unternehmen wird verpflichtet, die Anforderungen des KRITIS-Dachgesetzes und der noch zu erarbeitenden Rechtsverordnungen mit den konkreten Durchführungsbestimmungen umzusetzen.

Die Risikoanalysen werden rasch zu der Erkenntnis führen: Der regulierte KRITIS-Betrieb kann seine eigene Business Continuity nur dann erfolgreich managen, wenn auch seine wichtigsten Geschäftspartner (privat und staatlich) spezifische Mindestanforderungen im Bereich Business Continuity erreichen.

2. Welle:

Der regulierte KRITIS-Betrieb wird dann Mindestanforderungen für das Business Continuity Management (abgeleitet aus den eigenen Anforderungen) an seine Geschäftspartner bzw. in die Lieferkette weitergeben.

Damit würde sich die Reichweite des KRITIS-Dachgesetzes vervielfachen und eine fünf- bis sechsstellige Anzahl von Unternehmen müssten „plötzlich“ Resilienzmaßnahmen konzipieren, umsetzen und nachweisen.

Gerade kleine und mittlere Unternehmen dürften von den zu erwartenden einmaligen und laufenden Ausgaben überfordert werden.

Daher ist es wichtig, für bedürftige Unternehmen finanzielle Entlastungen (z.B. Sonderkredite und Sonderabschreibungen) vorzuhalten.

Und ganz wichtig: Der Zugang zu derartigen finanziellen Entlastungen darf NICHT daran geknüpft werden, ob es sich um ein reguliertes Unternehmen (vgl. Regelschwellenwert) handelt, sondern ob es sich um ein von der Implementierung des KRITIS-Dachgesetzes **betroffenes** Unternehmen handelt.

5 Grenzen klassischer Sicherheitskonzepte - wenn Schutz nicht gelingt

Die im KRITIS-Dachgesetz beschriebenen Maßnahmen orientieren sich am Allgefahrenansatz und fokussieren sich auf den Schutz vor Angriffen in der physischen Welt.

Die Diskussion der beschriebenen „Resilienzmaßnahmen“ fokussierte sich in den letzten beiden Jahren häufig auf Schutzmaßnahmen gegenüber sicherheitsbezogenen Herausforderungen - insbesondere im Bereich der Standortsicherheit.

Dass es bei der Umsetzung des Gesetzes um deutlich mehr geht, wird vielen betroffenen Organisationen vermutlich erst im Rahmen der Risikoanalysen (nach dem Allgefahrenansatz) und der Business Continuity Planung klar werden.

Wie im „Grünbuch Zivil-Militärische Zusammenarbeit 4.0“ des Zukunftsforum Öffentliche Sicherheit e.V. im Februar 2025 dargestellt, lassen sich Kritische Infrastrukturen nach ihrer „Schützbarkeit“ in drei Kategorien einteilen:

- Bei gut schützbaren Kritischen Infrastrukturen ist eine klassische Rundumsicherung (Zaun etc.) möglich und aufgrund ihrer räumlichen Lage sind sie im Falle einer Alarmierung durch Interventionskräfte (Polizei; Feuerwehr) gut und rasch erreichbar. Ein Beispiel hierfür wäre ein Rechenzentrum, dass in einer Stadt in der Nähe der einer Polizeidienststelle liegt.

- Auch bei eingeschränkt schützbaren Kritische Infrastrukturen ist die klassische Rundumsicherung (Zaun etc.) möglich, aufgrund ihrer räumlichen Lage sind sie im Falle einer Alarmierung durch Interventionskräfte (Polizei; Feuerwehr) jedoch weder gut noch rechtzeitig erreichbar, um einen Schaden zu verhindern oder zu begrenzen. Ein Beispiel hierfür wäre ein Umspannwerk in einer ländlichen Region irgendwo im Wald fernab der nächsten Siedlung.

- Bei den nicht wirklich schützbaren Kritischen Infrastrukturen ist aufgrund ihrer Art eine klassische Rundumsicherung nicht möglich. Sie sind schwer abgrenzbar und meist nicht umschließbar. Somit können potenzielle Täter üblicherweise ungehindert und unbemerkt an die Kritischen Infrastrukturen gelangen. Dort können sie ihre Tat meist ungestört beginnen und vollenden. Ein Zusammentreffen mit Interventionskräften müssen sie kaum fürchten. Beispiele für solche Infrastrukturen sind Autobahnen, Schienen, Hochspannungsleitungen, Tiefseekabel etc.

Wenn nun ein „Schutz“ im klassischen Sinn für viele Kritische Infrastrukturen nicht möglich ist, dann muss akzeptiert werden, dass dort Straftaten begangen werden, Schäden entstehen und der Betrieb der betroffenen Infrastruktur in der Folge eingeschränkt ist oder gar eingestellt werden muss.

Falls aber trotz „nicht aufzuhaltender“ Angriffe ein Betrieb Kritischer Infrastrukturen mit möglichst kurzen Ausfallzeiten oder gar eine unterbrechungsfreie Aufrechterhaltung der benötigten (Dienst-)Leistungen angestrebt wird, dann ist hierfür eine gute Business Continuity Planung mit angemessenen Redundanzen, Reserven und der Fähigkeit zur Schnellinstantsetzung erforderlich.

Das KRITIS-Dachgesetz sollte diesen Aspekt stärker hervorheben.

6 Resilienz vs. Effizienz

Die Business Continuity Planung für Kritische Infrastrukturen sollte stets auch die drei folgenden Themen berücksichtigen:

- Redundanzen u.a. im Sinne von alternativen Einrichtungen und Handlungsoptionen
- Reserven u.a. im Sinne von Lagerhaltung für den Geschäftsbetrieb
- Schnellinstantsetzung im Sinne einer raschen Schadensbeseitigung

All das stärkt die Resilienz - schwächt aber leider (zunächst) die Effizienz.

In den letzten rund 30 Jahren wurden die meisten Organisationen kontinuierlich auf Effizienz getrimmt, wobei eine stetige Schwächung der Resilienz akzeptiert wurde. Redundanzen, Reserven und Fähigkeiten zur Schnellinstantsetzung wurden aus Kostengründen abgebaut.

Das KRITIS-Dachgesetz sollte die Chance nutzen, auf eine Balance von Effizienz und Resilienz hinzuwirken.

Doch Resilienz kostet Geld - insbesondere, wenn nun auch strategische Geschäftsentscheidungen früherer Jahre in Bezug auf den Wert von Redundanzen, Reserven und die Fähigkeiten zur Schnellinstantsetzung vor dem Hintergrund der aktuellen Sicherheitslage hinterfragt werden.

Hier werden vermutlich geeignete Anreize erforderlich sein, damit künftig vermehrt in die Resilienz statt in die Effizienz investiert wird.

7 Konvergenz physischer und digitaler Sicherheit

Die Konvergenz der physischen und der digitalen Sicherheit ist seit über 20 Jahren ein Thema in den Großunternehmen. Organisatorische und prozessuale Lösungen hierfür wurden erarbeitet und in der Praxis erprobt.

Im Kern geht es darum, dass verteilte Zuständigkeiten im Unternehmen nicht dazu führen sollen, dass mögliche Angreifer Schwachstellen in Form von Abstimmungs- oder Regelungslücken erkennen, die sie für ihre Zwecke nutzen können.

In den Erläuterungen zu §14 Absatz 2 findet sich auf S. 58 folgender Hinweis:

„Soweit das Bundesamt für Sicherheit in der Informationstechnik branchenspezifische (...) Sicherheitsstandards (...) anerkannt hat, sollen diese um weitere Aspekte und Maßnahmen zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen ergänzt werden, um die Kohärenz zwischen IT-Sicherheit und Verpflichtungen nach dem KRITISDachG möglichst kohärent in den branchenspezifischen Resilienzstandards abzubilden und Doppelungen sowie gegebenenfalls Widersprüche zu vermeiden.“

Das KRITIS-Dachgesetz sollte diesen Aspekt (Konvergenz / Kohärenz) stärker hervorheben.