21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll
der 18. Sitzung

Innenausschuss
Berlin, den 1. Dezember 2025, 14:00 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 2 600

Vorsitz: Josef Oster, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 4**

a) Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/2510

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Wirtschaft und Energie
Verteidigungsausschuss
Verkehrsausschuss
Ausschuss für Digitales und Staatsmodernisierung

Berichterstatter/in:
Abg. Sebastian Schmidt [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Rasha Nasr [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Jan Köstering [Die Linke]

b) Antrag der Abgeordneten Dr. Konstantin von Notz, Jeanne Dillschneider, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Deutschland resilient machen – Für einen ganzheitlichen Schutz unserer kritischen Infrastruktur

BT-Drucksache 21/2725

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Verteidigungsausschuss
Ausschuss für Digitales und Staatsmodernisierung

Berichterstatter/in:
Abg. Sebastian Schmidt [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Rasha Nasr [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Jan Köstering [Die Linke]

Anwesende Mitglieder des Ausschusses

Fraktion	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Gregosz, David Hain, Heiko Oster, Josef Schmidt, Sebastian Strauss-Köster, Dr. Katja	
AfD	Janich, Steffen	
SPD	Baldy, Daniel Nasr, Rasha	
BÜNDNIS 90/ DIE GRÜNEN	Notz, Dr. Konstantin von	
Die Linke	Fey, Katrin Köstering, Jan	

Anwesende Mitglieder mitberatender Ausschüsse

Fraktion	Mitglied	Ausschuss
CDU/CSU	Schmidt, Henri	Verkehrsausschuss

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 1. Dezember 2025, 14.00 Uhr
„Kritis-DachG“

Stand: 1. Dezember 2025

Manuel 'HonkHase' Atug[4)]
Gründer und Sprecher der AG KRITIS

Alexander Averhoff[5)]
Deutscher Städte- und Gemeindebund (DStGB), Berlin

Mathias Böswetter[1)]
Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik - BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Berlin

Sylvia Borcherding[2)]
Geschäftsführerin Corporate Services - 50Hertz Transmission GmbH, Berlin

Prof. Dr. Clemens Gause[1)]
Geschäftsführer beim Verband für Sicherheitstechnik e.V. (VfS), Hamburg

Dr. Jürgen Harrer[2)]
Universität der Bundeswehr München, Center for Intelligence and Security Studies (CISS)

Prof. Dr. Dennis-Kenji Kipker[3)]
Universität Bremen, cyberintelligence.institute, Frankfurt am Main

Kerstin Petretto[1)]
Senior Managerin Sicherheit und Verteidigung - BDI Bundesverband der Deutschen Industrie e.V., Berlin

Christian Stuffrein[5)]
Deutscher Landkreistag und Deutscher Städtetag (DLT), Berlin

---

1) Vorschlag: Fraktion der CDU/CSU
2) Vorschlag: Fraktion der SPD
3) Vorschlag: Fraktion BÜNDNIS 90/DIE GRÜNEN
4) Vorschlag: Fraktion Die Linke
5) gemäß § 69a Absatz 2 GO-BT

Die Stellungnahmen zur Anhörung sind auf der Internetseite des Ausschusses abrufbar.

Beginn der Sitzung: 14.01 Uhr

Tagesordnungspunkt 1

a) Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/2510

b) Antrag der Abgeordneten Dr. Konstantin von Notz, Jeanne Dillschneider, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/ DIE GRÜNEN

Deutschland resilient machen – Für einen ganzheitlichen Schutz unserer kritischen Infrastruktur

BT-Drucksache 21/2725

Amt. Vors. **Josef Oster** (CDU/CSU): Meine sehr geehrten Damen und Herren, verehrte Kolleginnen und Kollegen, ich darf Sie am heutigen Nachmittag zum Einstieg in diese Sitzungswoche sehr herzlich zur 18. Sitzung unseres Innenausschusses begrüßen. Wir treffen uns heute im Rahmen einer öffentlichen Sitzung zur Anhörung von Sachverständigen. Das Thema unserer Anhörung heute ist der Gesetzentwurf der Bundesregierung zur Umsetzung der EU-Richtlinie 2022/2557 und zur Stärkung der Resilienz-kritischen Anlagen auf den Bundestagsdrucksachen 21/2510 und 21/2725.

Ich möchte ganz zu Beginn Ihnen, sehr geehrte Sachverständige, danken, dass Sie unserer Einladung gefolgt sind und dass Sie uns mit Ihrer Expertise zur Verfügung stehen und auch im Nachgang dann Fragen der Kolleginnen und Kollegen des Innenausschusses und der mitberatenden Ausschüsse beantworten werden. Ich begrüße zunächst die von den Fraktionen benannten und hier anwesenden Sachverständigen: Da sind in alphabetischer Reihenfolge Herr Manuel Atug, Herr Mathias Böswetter, Frau Sylvia Borcherding, Herr Prof. Dr. Clemens Gause, Herr Dr. Jürgen Harrer, Herr Prof. Dr. Dennis-Kenji Kipker und Frau Kerstin Petretto. Von den Kommunalen Spitzenverbänden darf ich Herrn Alexander Averhoff vom Deutschen Städte- und Gemeindebund und Herrn Christian Stuffrein vom Deutschen Landkreistag begrüßen – Sie vertreten heute hier auch den Deutschen Städtetag. Ich freue mich darüber hinaus, für die Bundesregierung die Parlamentarische Staatssekretärin Daniela Ludwig hier begrüßen zu dürfen – auch Ihnen ein herzliches Willkommen.

Ich darf darauf hinweisen, dass diese Sitzung live im Bundestagsfernsehen übertragen wird und auch auf unserer Homepage und ab morgen dann in der Mediathek des Deutschen Bundestages für die Öffentlichkeit zum Abruf bereitstehen wird. Wir hatten, wie üblich, vorab um schriftliche Stellungnahmen gebeten. Bei all jenen, die das gemacht haben und eine Stellungnahme abgegeben haben, darf ich mich bedanken. Darüber hinaus weise ich darauf hin, dass von dieser Sitzung ein Wortprotokoll erstellt wird und Ihnen dann zur Korrektur übersandt werden wird.

Für die Anhörung heute haben wir ein Zeitfenster von 14.00 bis maximal 16.00 Uhr vereinbart. Zu Beginn werde ich jedem Sachverständigen, jeder Sachverständigen die Gelegenheit geben, vielleicht ergänzend oder vertiefend zu der eingegangenen schriftlichen Stellungnahme, ein Eingangsstatement abzugeben, das möglichst nicht länger als drei Minuten dauern wird und ich bitte Sie, dies auch einigermaßen so einzuhalten. Danach werden wir in die Fraktionsrunden einsteigen. Wie sich die genau darstellen werden, werde ich nachher noch sagen. Ich würde dann zunächst einmal, wenn es keinen Widerspruch gibt, so einsteigen und mit den Sachverständigen beginnen. Wir machen auch das in alphabetischer Reihenfolge. Ich würde zunächst Herrn Atug um sein Eingangsstatement bitten. Bitte schön.

SV **Manuel Atug** (AG KRITIS): Vielen Dank, Herr Vorsitzender. Liebe Zuhörende, die AG KRITIS ist ein unabhängiger Zusammenschluss von Expert-Innen aus dem KRITIS-Umfeld. Unser einziges Ziel ist die Erhöhung der Versorgungssicherheit in der Bevölkerung. Die EU hat sich vor vielen Jahren durch die EU-CER-Directive sinnvolle Gedanken gemacht, wie wir kritische Infrastrukturen vor Unfällen oder Naturereignissen, vor gesundheitlichen Notlagen wie Pandemien, vor hybriden Bedrohungen und anderen feindlichen Bedrohungen wie terroristischen Straftaten, vor krimineller Unterwanderung und vor Sabotage schützen. Berücksichtigt werden sollen auch sektorübergreifende und grenzüberschreitende Risiken. Das alles erleben wir derzeit – der Schritt war also richtig. In Deutschland wurde aber ständig verzögert und herumgeeiert. Vorherige Stellung-

nahmen von Verbänden und der AG KRITIS selbst wurden im aktuellen Referentenentwurf vollständig ignoriert; das erreicht eine neue Größe von Ignoranz, besonders in diesen Zeiten der steigenden hybriden Gefährdungen und der Sicherheitsmeldungen, die wir hier täglich erleben – realitätsferner und verantwortungsloser kann man sich durch diese Haltung nicht aufstellen!

Verschiedene Einlassungen von BMI-Mitarbeitenden waren dahingehend eindeutig, dass das BMI zwischen den verschiedenen Entwürfen und Anhörungen explizit nicht beabsichtigte, irgendwas zu ändern. Vor allem Wirkmechanismen nachgeordneter Behörden wurden sogar durch das BMI unterbunden, um Handlungsdruck zu vermindern. Selbst betroffene Verbände äußerten sich uns gegenüber verständnislos, trauen sich das aber nicht laut zu sagen. Dieses Verhalten des BMI können wir nur als vorsätzliche Arbeitsverweigerung betrachten. Wir sind zu der Überzeugung gekommen, dass das BMI vorsätzlich Menschenleben gefährdet und auch riskiert, um internen Abstimmungs- und Arbeitsaufwand zu reduzieren. Die enthaltenen Sektoren, die im Gesetzentwurf stehen, sind höchst lückenhaft, der Sektor Staat und Verwaltung ist dekorativer Natur, jeder Schweizer Käse hat weniger Löcher als die in diesem Entwurf vorhandene Definition aufzeigt.

Die Bundesverwaltung wird minimal adressiert, Landes- und Kommunalverwaltungen sind von den Regelungen nicht betroffen. In § 22 des Gesetzentwurfes – „Ausnahmebescheid“ – wird diese Mangeldefinition noch weiter relativiert. Darüber hinaus fehlen relevante KRITIS-Sektoren wie Medien und Kultur, Großforschungseinrichtungen und die Chemiebranche – weiterhin sollen also Störfallbetriebe und kritische Industrie ungeschützt bleiben. Zentrale Regelungen sollen erst in zukünftigen Verordnungen in 2030 getroffen werden. KRITIS-Betreiber müssen dann die vorzunehmenden physischen Umbaumaßnahmen bewerten und budgetieren (2031), dann europaweit ausschreiben (2032), dann beauftragen (2033) und dann umsetzen (ungefähr 2033 bis 2040).

Darüber hinaus ist der Schwellenwert erneut auf den nicht wissenschaftlich ermittelten Daumenwert „Versorgung von 500 000 Personen“ gesetzt worden – wer also von KRITIS abhängig ist, die weniger Menschen versorgt, hat Pech gehabt und erhält im Störfall keine Versorgung, ist also auf sich selbst gestellt. Das Grundgesetz sieht aber eine Daseinsvorsorge vor und eine Gleichheit aller Menschen. Wir betonen daher noch einmal, dass durch eine solche Vorgehensweise vorsätzlich Menschenleben riskiert werden, wenn keine Anpassung zu diesen erheblichen Mängeln erfolgt. Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Atug. Wir fahren fort mit Herrn Averhoff, bitte schön.

SV **Alexander Averhoff** (DStGB): Sehr geehrter Herr Oster, sehr geehrte Damen und Herren. Vielen Dank für die Gelegenheit, hier die Position des Deutschen Städte- und Gemeindebundes darlegen zu können. Wir haben eine Stellungnahme zugesandt und ich möchte einige Punkte aufgreifen und Ihnen noch einmal kurz ans Herz legen: Zum einen ist aus unserer Sicht eine enge kommunale Einbindung notwendig. Dafür bietet das KRITIS-Dachgesetz zwei Möglichkeiten. Das ist einmal die Erarbeitung der nationalen KRITIS-Resilienz-Strategie, die, wenn wie beschrieben umgesetzt wird, schon Mitte Januar fertig sein soll. Vielleicht wird es etwas später, vielleicht besteht da noch die Möglichkeit, die kommunale Ebene mit hineinzunehmen. Und ganz wichtig ist das auf Seite 41 genannte Ständige Beratungsgremium. Da sind aktuell Länder und Wirtschaft genannt. Die Kommunen sind eingeklammert. Da würden wir uns wünschen, die Klammern herauszunehmen und die kommunalen Spitzenverbände einzubinden, um eine langfristige Kommunikation zu ermöglichen und auch hinsichtlich der Evaluierung einfach eine gute Kommunikation gewährleisten zu können.

Zum Sektor Staat und Verwaltung ist schon etwas gesagt worden. Auch wir sehen das kritisch, dass die Kommunen komplett herausgenommen sind und dass das in einer Pauschalität geschieht, die auch Einzelfälle erst einmal nicht zulässt. Da haben wir eine andere Meinung: Staat und Verwaltung sind Grundpfeiler der Daseinsvorsorge. Da wünschen wir uns eine klare Definition, um die Funktionsfähigkeit kommunaler Verwaltung im Krisenfall gewährleisten zu können. Und da stellt sich auch die Frage, wenn ein Betreiber kritischer Infrastruktur in einer Kommune ansässig ist, ob da nicht automatisch eine gewisse Betroffenheit hergestellt ist. Dazu sagt das Gesetz aber nichts.

Dann dritter Punkt: Die Umsetzungsfristen sind für uns zu kurz. Das haben wir auch schon im Sommer gegenüber dem Referentenentwurf angemerkt. Da

wünschen wir uns eine Verlängerung auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) meist genutzten 24 Monate. Und zum Punkt der Schwellenwerte und Kleinbetreiber möchte ich auch noch etwas sagen: Kleinere Betreiber sind ganz fraglos auch sicherheitsrelevant. Wir halten es aber für nicht ideal, ganz kurzfristig den Schwellenwert deutlich zu senken, sondern würden das zu einem späteren Zeitpunkt vornehmen. Das könnte auch im Rahmen der Evaluierung oder eines Zwischenberichtes geschehen. Aber nun sehr kurzfristig auf irgendwie gegriffene Werte abzusenken, das sehen wir kritisch, würden uns aber freuen, wenn es dennoch auch für kleinere Betreiber Unterstützungsangebote des Bundes gäbe, sodass sie mitgenommen werden, aber nicht direkt mit weiteren Auflagen versehen werden. Denn – das wissen Sie sicherlich – wir haben eine sehr angespannte kommunale Finanzlage. Das letzte Jahr hat minus 24 Milliarden Euro gebracht, das laufende ein Defizit von um die 30 Milliarden Euro. Schon jetzt helfen kommunale Unternehmen durch Gewinnabführungen dabei, die kommunalen Haushalte zu stützen. Das würde mit dem Fragezeichen versehen werden, wenn wir nun die gleichen Unternehmen wieder belasten. Deshalb, ja, gerne Unterstützungsangebote, aber obligatorische Vorgaben zum jetzigen Zeitpunkt vielleicht nicht. Für die Finanzierbarkeit, die natürlich auch sehr wichtig ist, der Hinweis auf das Grundgesetz, aber das macht ja auch schon der Gesetzentwurf. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Averhoff. Es geht weiter mit Herrn Böswetter.

SV **Mathias Böswetter** (BDEW): Sehr geehrter Herr Vorsitzender Oster, sehr geehrte Damen und Herren Abgeordnete, sehr geehrte Staatssekretärin Ludwig, meine Damen und Herren. Vielen Dank, dass sich der Bundesverband der Energie- und Wasserwirtschaft heute hier im Rahmen dieses Ausschusses, dieser öffentlichen Anhörung zum KRITIS-Dachgesetz äußern kann. Der Bundesverband der Energie- und Wasserwirtschaft und seine Landesorganisationen vertreten über 2 000 Mitgliedsunternehmen der Strom-, Gas-, Wärme- sowie Wasser- und Abwasserwirtschaft in Deutschland. Die Mitgliedsunternehmen des BDEWs sichern damit rund 90 Prozent des Strom- und über 95 Prozent des Netzbetriebs sowie etwa 80 Prozent der Trinkwasserversorgung in Deutschland. Resiliente, kritische Infrastrukturen der Energie- und Wasserwirtschaft sind deshalb auch eine Grundvoraus-setzung für das Funktionieren aller Lebensbereiche. Ohne eine verlässliche Versorgung mit Energie und Wasser funktionieren weder Industrie, weder Dienstleistungen noch die öffentliche Daseinsvorsorge. Das KRITIS-Dachgesetz schafft erstmals einen sektorübergreifenden Rechtsrahmen für physische Sicherheit von Resilienz-kritische Anlagen und ergänzt das bestehende IT-Sicherheitsrecht. Hier ist es wichtig, festzustellen: Für uns, für den BDEW, ist für den Energiesektor die Verzahnung mit dem IT-Sicherheitsrecht zielführend und gut gelöst. Der Entwurf, der uns vorliegt, baut auf bewährten Strukturen, insbesondere der IT-Sicherheitskataloge der Bundesnetzagentur, auf und setzt bei jenen Betreibern an, die im Rahmen von NIS-1 bereits Erfahrungen mit Risikomanagement, Beschaffung, personeller Sicherheit und vor allem den teilweise sehr aufwendigen Nachweispflichten im Rahmen von Zertifizierungsprozessen gesammelt haben. Genau vor diesem Hintergrund sehen wir auch eine grundsätzliche Herabsetzung des Regelschwellenwertes besonders kritisch. Die Betreiber, die über keine vergleichbare Erfahrung verfügen, werden durch die Umsetzung sehr wahrscheinlich überfordert, wenn der Regelschwellenwert deutlich herabgesetzt wird; auch sind sie die letzten Jahre mit anderen Erwartungen in eine Umsetzung gegangen – nämlich, dass sie nicht betroffen sein würden.

Für eine effektive und nachhaltige Umsetzung des KRITIS-Dachgesetzes ist aus unserer Sicht und aus Sicht der Energie- und Wasserwirtschaft Folgendes entscheidend: Wir brauchen erstens keine pauschale Herabsetzung des Regelschwellenwertes im Gesetz, zweitens Transparenz beim Erfüllungsaufwand und Regelungen, die eine verlässliche Refinanzierung der Resilienz-Maßnahmen ermöglichen, drittens ein umfassendes Lagebewusstsein und eben auch eine Stärkung des bidirektionalen Informationsaustausches zwischen Behörden und Betreibern von kritischer Infrastruktur, viertens den wirksamen Schutz sicherheitsrelevanter Informationen – das heißt eben auch eine Neubewertung der Transparenzpflichten – und fünftens darf der Bund die Betreiber bei der akuten Drohnenbedrohung, die wir gerade sehen, nicht alleinlassen. Die Betreiber dürfen durch das KRITIS-Dachgesetz nicht de facto zu etwas verpflichtet werden, was sie nicht dürfen. Deshalb: Drohnenabwehr muss hoheitliche Aufgabe

bleiben und mit geeigneten Zuständigkeiten und Systemen für eine effektive Drohnenabwehr in der Fläche hinterlegt werden. Vielen lieben Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank, Herr Böswetter. Es geht weiter mit Frau Borcherding, bitte schön.

SVe **Sylvia Borcherding** (50Hertz): Vielen Dank, dass ich heute die Gelegenheit habe, als Sachverständige die Meinung von 50Hertz zu vertreten. Wir sind einer der vier Übertragungsnetzbetreiber in Deutschland und somit unbedingt kritische Infrastruktur. Und ich möchte zunächst einmal sagen, dass wir das KRITIS-Dachgesetz als bundeseinheitlichen Rahmen unbedingt begrüßen und auch als einen längst überfälligen Schritt begrüßen. Es ist aus unserer Sicht ein ganz wichtiger Meilenstein zur Stärkung der Resilienz gegenüber sowohl physischen als auch hybriden Bedrohungen und setzt entsprechend die EU-CER-Richtlinie um.

Es gibt drei Aspekte, wo wir noch dringenden Nachbearbeitungsbedarf sehen: Das eine ist in Bezug auf die Transparenzpflichten, und zwar haben wir Stand heute Veröffentlichungspflichten, die Informationen in einem Detail von uns in der Veröffentlichung verlangen, die es mit den heutigen technologischen Methoden, also künstlicher Intelligenz oder Systemen, die Informationen aggregieren und entsprechend analysieren, Aggressoren extrem leicht machen, sich eine Übersicht über unsere Infrastrukturen zu verschaffen und eben auch die entsprechenden Angriffspunkte zu identifizieren. Diese Art der Bedrohungslage ist bisher im Gesetzentwurf noch nicht ausreichend berücksichtigt. Daher fordern wir eine ganzheitliche Neubewertung und Anpassung der Transparenzpflichten, und zwar in Bezug auf die Detaillierung – da können wir uns auch andere Möglichkeiten vorstellen.

Der zweite Aspekt sind die Finanzierung und Kosten, von denen wir uns wünschen, dass sie klar geregelt werden. Die Resilienz-Maßnahmen, die notwendig sind bei Netzen, die in Friedenszeiten entstanden sind, verursachen erhebliche zusätzliche Investitions- und Betriebskosten, sowohl, was die physische Sicherung betrifft, als auch die IT-Sicherheit, Redundanzen, Frühwarnsysteme im Sinne der Detektion. Wir brauchen für uns Klarheit, welche Kosten anerkannt werden und vor allen Dingen auch wie neue Technologien und langfristige Betriebskosten entsprechend berücksichtigt werden. Daher fordern wir einen verbindlichen, bundesweit einheitlichen Rahmen zur Anerkennung und Refinanzierung von Resilienz-Kosten, auch um Planungssicherheit zu gewährleisten.

Der dritte Aspekt bezieht sich auf die maritime Sicherheit und die Koordination der maritimen Sicherheit. Es ist geplant, dass das Maritime Sicherheitszentrum heute schon, aber auch in Zukunft eine wesentliche Rolle bei der Lageidentifizierung spielt. Wir haben aber heute in der Tat zersplitterte Zuständigkeiten und würden daher empfehlen, dass auch das Maritime Sicherheitszentrum an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) berichtet, sodass wir eine gemeinsame Lage übergreifend identifizieren können. Und in dem Zusammenhang auch noch mal der wichtige Hinweis der Zwei-Wege-Kommunikation: Wir können uns als kritische Infrastruktur nur vorbereiten, wenn wir wissen, wie die Lage aussieht und wir Gelegenheit haben, auch entsprechende Bereitschaften sicherzustellen. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank, Frau Borcherding. Wir fahren fort und das Wort hat jetzt Prof. Dr. Gause.

SV **Prof. Dr. Clemens Gause** (VfS): Vielen Dank. Vielen Dank auch für die Einladung, dass wir als Verband für Sicherheitstechnik eingeladen worden sind. Der Verband für Sicherheitstechnik besteht seit weit über 30 Jahren. Wir sind Normierer und Standardisierer genau in dem Teil, der in der CER-Richtlinie so brennend interessiert, nämlich die physische Sicherheit, die man ganz bei der EU-Kommission, als man die CER, glaube ich, geschaffen hat, so ein bisschen hat unter den Tisch fallen lassen; vielleicht war „Cyber“ auch irgendwie zu vordringlich. Aber was nützt einem die Cybersicherheit in einem Rechenzentrum, wenn man in das Rechenzentrum auch einfach einsteigen kann? Also: Physische Sicherheit ist wichtig, ist elementar!

Wir freuen uns sehr über diesen Gesetzentwurf, weil er in die richtige Richtung geht, das muss man ganz klar adressieren. Wichtig auch: Es gibt Normierungen und Standards, die seit vielen Jahren erprobt sind, die immer wieder erweitert werden. Da, wie gesagt, gibt es Handbücher, die wir herausgeben. Da ist ganz viel Material da, was wir jetzt in Gang bringen können. Und in Anschluss an meine Vorredner möchte ich hier einen ganz wichtigen Punkt setzen:

Uns ist ganz wichtig, dass wir hier vor allem die Sicherheitswirtschaft nach vorne bringen. Wenn wir vielleicht in anderen Wirtschaftsbereichen schwächeln, so wäre es doch eine gute Idee, wenn wir hier Sicherheit, nicht nur Sicherheitstechnik, sondern generell die Sicherheitswirtschaft mit dem, was zum Beispiel in den §§ 13, 14 des Gesetzentwurfs vorhanden ist, nach vorne bringen und wir vor allem hier die Unternehmen, die, wie meine Vorredner auch schon angedeutet haben, dann in der Betreiberpflicht sind, vor allem erstmals sind, hier mitnehmen und sie vielleicht über Wirtschaftshilfen unterstützen. Wir denken vielleicht an Steuererleichterungen oder an vielleicht direkte Subventionen, vielleicht auch in dem einen oder anderen speziellen Fall sogar an direkte Haushaltsmittel, die zur Verfügung gestellt werden müssten oder sollten, um hier als Idee auch einen Wirtschaftsfaktor in Deutschland zu errichten.

Und das könnte man vielleicht jetzt nicht in dem ersten Entwurf, den wir ja doch jetzt durch die Tür bringen wollen, formulieren, aber vielleicht in nachgelagerten Gesetzesmaterien spätestens bei der Evaluation. Insgesamt sind wir sehr dafür. Und wir sind auch dafür, das BBK weiterhin zu stärken. Wir stehen bereit, mit entsprechenden Standards hier sozusagen ähnlich wie beim „BSI-Standard“ einen „BBK-Standard“ zusammenzustellen und gegebenenfalls auch neue Normierungen ins Leben zu rufen. Wie gesagt, es ist viel da. Wir freuen uns sehr über diesen Gesetzentwurf und wünschen uns, dass er möglichst gut und bald „durch die Tür kommt“.

Amt. Vors. **Josef Oster** (CDU/CSU): Genau das ist der Auftrag, den wir als Parlamentarier haben, das möglichst bald im Plenum zum Finale zu bringen – schauen wir einmal. Vielen Dank, Herr Gause. Es geht weiter mit Dr. Harrer, bitte.

SV **Dr. Jürgen Harrer** (CISS): Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, vielen Dank für die Gelegenheit, hier im Innenausschuss zur Stärkung der Resilienz-kritischen Anlagen Stellung zu nehmen. Folgende Themen möchte ich adressieren: Thema 1, Erfüllungsaufwände und weitere Kosten. Die neuen Resilienz-Anforderungen im Bereich der Sicherheit, vor allem der Standortsicherheit, werden bei vielen betroffenen Betreibern zu hohen einmaligen und laufenden Kosten führen. Gerade die kleinen und mittleren Betriebe sollten nicht überlastet werden. Deswegen wäre finanzielle Unterstützung sinnvoll, zum Beispiel in Form von Sonderkrediten und Sonderabschreibungen. Und natürlich ist zu erwarten, dass sowohl die einmaligen als auch die laufenden Kosten auf die Leistungen umgelegt und an die Bürgerinnen und Bürger weiterverrechnet werden.

Thema 2, individuelle und kollektive Resilienz. Im Gesetzentwurf sind vor allem individuelle Resilienz-Maßnahmen für ein Mindestmaß an Resilienz in jedem regulierten Unternehmen dargestellt. Für das Funktionieren des Gesamtsystems von KRITIS-Organisationen, privaten und staatlichen, wird es darauf ankommen, die kollektive Resilienz aller Beteiligten zu stärken. Sinnvoll hier wäre eine überregionale Steuerungsfunktion und auch eine Plattform zur Bedrohungsfrüherkennung, wie sie im Eckpunktpapier zur Nationalen Wirtschaftsschutzstrategie auch angedacht ist, eben für einen wechselseitigen bilateralen Austausch relevanter Informationen zwischen Behörden und Unternehmen. Auch die Fähigkeit, ein interdisziplinäres Lagebild in Echtzeit zu erzeugen, das die Lageführung bei parallelen Ereignissen und überregionalen Ereignissen unterstützt, wäre an dieser Stelle hilfreich.

Thema 3, Orientierungswert statt Regelschwellenwert. Eine echte Resilienz der Gefahrengemeinschaft von Staat, Wirtschaft und Bürgern kann nur dann gelingen, wenn sich alle Akteure in angemessener Weise daran beteiligen. Der Regelschwellenwert von 500 000 sendet womöglich die Botschaft, die großen Betreiber müssen sich schützen, alle anderen nicht – das wäre ein fatales Signal! Tatsächlich finden sich in § 5 des Gesetzentwurfs noch weitere Kriterien. Um Missverständnisse zu vermeiden, wäre es daher sinnvoll, den Begriff „Regelschwellenwert“ durch den Begriff „Orientierungswert“ zu ersetzen, wenn bei einer angestrebten sachgerechten Bestimmung eine Einzelfallbetrachtung unter Berücksichtigung mehrerer unterschiedlicher Kriterien vorgesehen ist. Das wäre der richtige Weg.

Implementierung in zwei Wellen. Dies sehen wir kommen. Eine niedrige vierstellige Anzahl von Unternehmen wird in der ersten Welle verpflichtet sein, die Anforderungen des KRITIS-Dachgesetzes umzusetzen. Dann werden diese KRITIS-Betriebe rasch erkennen, dass sie für ihre eigene Business Continuity auch die Business Continuity ihrer wichtigsten Geschäftspartner, privat und staatlich, benötigen. Deswegen wird es in einer zweiten Welle dazu kommen, dass Business Continuity Manage-

ment- (BCM-) Mindestanforderungen an die Geschäftspartner, an die Lieferkette weitergegeben werden. Damit kann sich die Reichweite des KRITIS-Dachgesetzes vervielfachen und eine fünf- bis sechsstellige Anzahl von Unternehmen müssen plötzlich Resilienz-Maßnahmen nachweisen. Gerade die kleinen und mittleren werden da wieder kostenmäßig überfordert und bräuchten finanzielle Entlastungen. Und ganz wichtig, der Zugang zu derartigen finanziellen Entlastungen darf nicht daran geknüpft sein, ob sich um ein reguliertes Unternehmen handelt, sondern um ein Unternehmen, das von der Implementierung betroffen ist.

Und zu guter Letzt, ganz kurz: Es gibt Infrastrukturen, die kann man in der Rundum-Sicherung nicht schützen. Da versagt alles, was wir bisher zu dem Thema wissen. Deswegen müssen wir das Augenmerk auf Business Continuity-Planung mit Reserven, Redundanz und der Fähigkeit zur Schnellinstandsetzung verlagern. Und das muss auch im Gesetz angemessen berücksichtigt sein! Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Es geht weiter mit Prof. Dr. Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Sehr geehrter Herr Vorsitzender, sehr geehrte Ausschussmitglieder, sehr geehrte Damen und Herren. Vielen Dank für die Einladung und die Möglichkeit, hier heute Stellung nehmen zu können. Kritische Infrastrukturen, die zentralen Versorgungs- und Funktionssysteme unseres Gemeinwesens, sind seit Jahren einer erheblich zunehmenden Gefährdungslage ausgesetzt. Parallel dazu bestehen bislang deutliche Regelungslücken: Während im Bereich der digitalen Infrastruktur mit den nationalen IT-Sicherheitsgesetzen 1 und 2 sowie auf europäischer Ebene mit NIS-1 und -2 bereits Regelungen geschaffen wurden, unterliegt die physische Infrastruktur bislang noch keinen eigenständigen Schutzvorgaben. Der deshalb vorgelegte Entwurf für ein KRITIS-Dachgesetz bleibt jedoch 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 Betreiber kritischer Infrastruktur 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 Infrastruktur tatsächlich gerecht werden kann. Nur ein solches konsistentes und einheitliches Gesamtgefüge vermag die Resilienz kritischer Infrastruktur nachhaltig zu stärken und den bestehenden Bedrohungen angemessen zu begegnen!

In diesem Zusammenhang möchte ich insbesondere gerne folgende Punkte hervorheben, die ich auch in meiner Stellungnahme ausführlicher adressiert habe. Die öffentliche Verwaltung, einschließlich wesentlicher Teile der Bundes-, Landes- und Kommunalverwaltung, bleibt weitgehend vom Anwendungsbereich ausgeschlossen. Das führt zu einem fragmentierten Schutzniveau. Die im KRITIS-Sektor Staat und Verwaltung vorhandenen Infrastrukturen sollten jedoch denselben Resilienz-Anforderungen unterliegen wie Anlagen privater Betreiber. Der vorliegende Entwurf enthält bislang kaum materielle Vorgaben dazu, welche konkreten Resilienz-Maßnahmen betreiberkritische Anlagen zu ergreifen haben. Konkrete, unmittelbar aus dem Gesetz ableitbare Handlungsanweisungen für Betreiber kritischer Infrastruktur fehlen somit weitestgehend. Im Mittelpunkt stehen überwiegend Zuständigkeits- und Verordnungsermächtigungen, und damit wird der Beginn substanzieller Anforderungen auf einen späteren Zeitpunkt verschoben. Die Verteilung der Zuständigkeiten zwischen BBK, BSI, Fachaufsichten und Landesbehörden ist im vorgelegten Gesetzentwurf unklar und birgt das Risiko divergierender Vollzugspraxis. Zudem fehlen Regelungen für einen einheitlichen, strukturierten Datenaus-tausch und eine zentralisierte Meldestelle. Die vorgeschlagene Meldepflicht droht aufgrund unklarer Abgrenzungen und weiteren parallel bestehender Meldewege zu erheblichem Aufwand für die betroffenen Unternehmen zu führen. Ein strukturierter Rückkanal, etwa in Form von Lagebildern, Warnhinweisen oder Empfehlungen fehlt bislang. Trotz inhaltlicher Schnittmengen bestehen weiterhin erhebliche Divergenzen zwischen der NIS-2-Umsetzung und dem KRITIS-Dachgesetz, die sich in der Praxis als problematisch erweisen. Unterschiedliche Begriffs-

verwendungen sowie abweichend ausgestaltete Anforderungen erschweren eine konsistente Betroffenheitsprüfung und führen zu einer vermeidbaren zusätzlichen Komplexität. Der vorliegende Entwurf des KRITIS-Dachgesetzes ist somit zwar ein wichtiger, aber bislang leider immer noch unvollständiger Schritt hin zu einem kohärenten Schutz kritischer Infra-strukturen in Deutschland. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kipker. Es geht weiter mit Frau Petretto. Bitte schön.

SVe **Kerstin Petretto** (BDI): Vielen Dank. Vielen Dank, Herr Vorsitzender, vielen Dank, Frau Staatssekretärin, sehr geehrte Damen und Herren, sehr geehrte Abgeordnete. Wirtschaftliche Resilienz ist *ein* zentraler Bestandteil unserer nationalen Sicherheit. Das KRITIS-Dachgesetz ist daher keine klassische Regulierung, sondern es ist tatsächlich ein elementarer sicherheitspolitischer Baustein. Unser gemeinsames Ziel ist klar: Resilienz erhöhen, ohne unnötige Bürokratie zu erzeugen. Es ist aus Sicht des Dachverbandes der Deutschen Industrie, des BDI, zentral, dass das Dachgesetz kommt. Nicht nur wegen der bereits gerissenen Frist, sondern weil wir alle dringend Rechtssicherheit brauchen. Gerade weil Staat und Wirtschaft gemeinsam für die nationale Sicherheit Verantwortung tragen, braucht es hier aber ein neues Mindset der Zusammenarbeit. Wir müssen weg von diesen extrem kurzen Stellungnahmefristen, die wir alle erfahren haben, endlich hin zu einer echten Partnerschaft im Sicherheitsbereich. Wir brauchen einen strukturierten Austausch in beide Richtungen, wir brauchen eine frühzeitige Einbindung der Expertise aus der Praxis, wenn es darum geht, neue Gesetze, neue Regulierungen zu schaffen, um gemeinsam unsere Sicherheit zu erhöhen. Unsere Idealvorstellung, das haben wir sehr oft platziert, war eine echte Verzahnung des NIS-2-Umsetzungsgesetzes und dem KRITIS-Dachgesetz. Gelandet sind wir jetzt bei zwei Gesetzen, nur in Teilen harmonisiert – das geht eigentlich besser.

Da aber ein erneutes Aufschnüren die Umsetzung weiter verzögern würde, möchte ich für heute erst einmal drei Punkte hervorheben, die aus unserer Sicht *jetzt* dringend nachgebessert werden müssen: Erstens, Staat und Wirtschaft sind Teil der kritischen Infrastruktur. Private Betreiber tragen einen Großteil der Grundversorgung der Bevölkerung; ebenso in der Verantwortung ist aber der Staat. Er muss funktionierende Abläufe und seine Handlungsfähigkeit sichern. Beide brauchen daher ein sehr hohes Schutzniveau. Und es ist daher nicht nachvollziehbar, warum große Teile der Bundes- und Landesverwaltung aus dem Dachgesetz ausgenommen worden sind. Eine wirklich überzeugende Begründung dafür hat tatsächlich auch noch niemand wirklich liefern können. Kosten können eigentlich kein Argument sein angesichts der laufenden hybriden Angriffe. Sie erinnern sich sicher an die Beiträge der Herren Selen und Jäger und von Frau Rosenberg kürzlich hier in diesem hohen Hause. Wir müssen hier vorankommen und der Staat ist ein Teil der kritischen Infrastruktur – diese Lücke gehört also geschlossen!

Zweitens fehlt in dem Gesetz die personelle Dimension. In vielen KRITIS-Sektoren fehlt eine gesetzliche Grundlage, wie Unternehmen überhaupt rechtssicher prüfen lassen können, ob Personen, die für physische und digitale Sicherheit im Rahmen des NIS-2-Umsetzungsgesetzes und des KRITIS-Dachgesetzes zuständig sind, zuverlässig und vertrauenswürdig sind. Das ist aber die Basis, weil diese Menschen brauchen wir und wir müssen sie prüfen. Es braucht daher einen rechtlichen Rahmen für eine freiwillige, staatlich durchgeführte Vertrauenswürdigkeitsüberprüfung. Der BDI hat hierzu bereits im März 2024 einen Vorschlag vorgelegt, den lasse ich Ihnen gerne im Nachgang noch einmal zukommen. Das ist tatsächlich ein Punkt, der offen ist.

Drittens werden die neuen Bedrohungen nicht adressiert, obwohl wir das KRITIS-Dachgesetz schon sehr lange diskutieren. Wenn zu einem relevanten Angriffssektor eine Rechtslücke besteht, dann darf man das nicht ausblenden. Ich spreche von den Drohnenüberflügen. Wir müssen hier regeln, wir brauchen klare Regeln für Detektionsstörungen und gegebenenfalls Abwehr durch Behörden oder auch unter klar definierten Bedingungen durch Unternehmen. Ich komme zu einem Punkt und freue mich auf die Diskussion.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Genau darum geht es. Wir machen das Finale in dieser Expertenrunde mit Herrn Stuffrein. Bitte schön.

SV **Christian Stuffrein** (DLT): Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete, herzlichen Dank für die Einladung,

um hier auch die kommunale Perspektive in den Prozess einbringen zu können; bei der Anhörung zum NIS-2-Umsetzungsgesetz wäre das aus unserer Sicht auch angezeigt gewesen. Vorneweg, ich vertrete wie auch ausgeführt heute den Deutschen Landkreistag und den Deutschen Städtetag. Wir begrüßen ausdrücklich, dass der Gesetzgeber mit dem KRITIS-Dachgesetz verbindliche nationale Regeln zum physischen Schutz für Betreiber kritischer Infrastrukturen schaffen möchte. Eine enge Verzahnung mit den Anforderungen zur Informationssicherheit ist dabei notwendig. Resilienz-Strategien, umfassende Prävention und effektiver Katastrophenschutz werden uns dabei in den kommen-den Jahren als gesamtstaatliche Mammutaufgabe begleiten. Die Kommunen sind dabei essentiell für die Handlungsfähigkeit des Staates. Der Großteil der Verwaltungsleistung für die Bürger, Unternehmen sowie die Bewältigung von Krisenlagen, Covid-19, Tierseuchen etc., werden hier erbracht. Ergänzend kommen neue Aufgaben im Bereich des „Operationsplans Deutschland“ auf die Kommunen zu. Der Bund sei gut geschützt, aber für das Leben der Menschen nicht zu kritisch, erläuterte auch der ehemalige Vizepräsident des BSI, Dr. Schabhüser. Auf Basis der ausgeführten Bedeutung der Kommunen sehen wir es als problematisch an, dass im Gesetz-entwurf der Bundesregierung gleich der komplette Sektor Staat und Verwaltung fehlt. Es benötigt hier dringend eines gemeinsamen Handelns von Bund und Ländern, um die Kommunen endlich einzubinden, eine kommunale Betroffenheit während seiner Ausgestaltung genauer zu eruieren, vorstellbar wäre die Aufnahme der Kernverwaltung. Die Umsetzung von Resilienz-Maßnahmen betrachten wir dabei schon heute als organisationseigene Aufgabe, benötigen aber entsprechende Unterstützung des Bundes und der Länder. Ergänzend fordern wir, dass die Rechtsverordnung gemäß § 4 Absatz 3 und § 5 Ab-satz 1 des Gesetzentwurfs so schnell wie möglich vorgelegt wird. Diese Regelung ist für die weitere Planung in den Kommunen entscheidend. Den angesetzten Schwellenwert von 500 000 versorgten Einwohnern bewerten wir als viel zu hoch. Damit würde das Gesetz keine Anwendung für Einrichtungen in der deutlichen Mehrheit der Kommunen entfalten. Denkbar ist der vom Bundesrat eingebrachte Schwellenwert von 150 000 versorgten Einwohnern.

Die Umsetzung der zahlreichen Anforderungen aus dem KRITIS-Dachgesetz erfordert weiterhin den Aufbau von Managementsystemen bei vielen Betreibern kritischer Anlagen. Hierfür ist eine Verlängerung der Frist in § 8 Absatz 7 auf 24 Monate notwendig. Darüber hinaus begrüßen wir das von der Bundesregierung geplante Ständige Beratungsgremium. Die Städte und Landkreise müssen in ihrer Funktion als Katastrophenschutzbehörden und Träger der KRITIS-relevanten kommunalen Wirtschaftsunternehmen zwingend Teil dieses Gremiums sein. Die kommunale Einbindung ist ergänzend auch für das geplante Meldewesen nach § 18 sicherzustellen.

Nun komme ich zum letzten Punkt. Für das ganzheitliche Resilienz-Management gehört der essentielle und wichtige § 13 des vorliegenden Gesetzentwurfes zwingend um Vorbereitungs- und Nachbereitungsmaßnahmen ergänzt. Ausgefallene kritische Infrastrukturen können Folgen mit sich bringen, die nicht durch den Katastrophenschutz vor Ort ersetzt werden können. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Stuffrein. Wir haben damit die Eingangsstatements abgeschlossen und kommen zu den Fraktionsrunden, die sich wie folgt darstellen: Wir werden von Fraktion zu Fraktion wechseln. Jede Fraktion hat zwei Minuten Zeit, bis zu zwei Fragen zu stellen. Es können sich zwei Fragen an einen Sachverständigen richten oder auch je eine Frage an zwei Sachverständige. Ich darf die Kolleginnen und Kollegen bitten, zu Beginn auch konkret zu benennen, an wen sich die Frage richtet, damit nicht alle immer in Hab-Acht-Stellung sein müssen. Die Antwort erfolgt unmittelbar auf die Frage und auch die Sachverständigen haben zwei Minuten je Frage Zeit, zu antworten. Wir starten mit der CDU/CSU-Fraktion. Das Wort hat der Kollege Schmidt. Bitte schön.

Abg. **Sebastian Schmidt** (CDU/CSU): Herr Vorsitzender, meine Damen und Herren. Ich habe eine Frage an zwei Sachverständige, nämlich an Herrn Averhoff vom DStGB und auch an Herrn Böswetter vom BDEW: In den unterschiedlichen Stellungnahmen wurde immer wieder auf den Regelschwellenwert Bezug genommen, auch hier in den mündlichen Stellungnahmen. Zuletzt hat der Bundesrat eine Absenkung dieses Schwellenwerts auf 150 000 Einwohner gefordert und meine Frage an Sie ist angesichts der Eilbedürftigkeit des Gesetzes: Wie bewerten Sie die Fähigkeit potenziell betroffener Unternehmen, insbesondere von KMU (Kleinstunternehmen, kleine und mittlere Unternehmen)

und jene in kommunaler Hand, die Anforderungen des Dachgesetzes zu erfüllen, wenn der Regelschwellenwert deutlich herabgesenkt wird?

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Schmidt. Es geht zur Beantwortung. Zunächst hat Herr Averhoff für bis zu zwei Minuten die Möglichkeit, das zu beantworten, dann Herr Böswetter. Herr Averhoff, bitte.

SV **Alexander Averhoff** (DStGB): Ja, Herr Abgeordneter Schmidt, vielen Dank für die Frage. Wir haben das in den zuständigen Gremien diskutiert und die Rückmeldungen waren sehr eindeutig, dass zum jetzigen Zeitpunkt eine Absenkung sehr kritisch gesehen wird – das aus den voran genannten Gründen der ohnehin schon sehr belasteten kommunalen Haushalte, worauf sich die Senkung auswirken würde. Wenn ich die kommunalen Unternehmen belaste, dann können diese nicht mehr auf die kommunalen Haushalte entlastend wirken. Und auch vor dem Gesichtspunkt – generell, wir reden immer viel von Bürokratieabbau und Unternehmen weniger belasten – wäre das zweifellos eine zusätzliche Belastung, für die das Gesetz zum jetzigen Zeitpunkt keine Gegenfinanzierung vorsieht. Das war einer meiner letzten Punkte im Eingangsstatement: Der Entwurf spricht es an, er lässt aber die Lösung offen. Er verweist auf die Bereichsausnahme, also das Finanzierungstool wird genannt, aber nicht näher darauf eingegangen. Das bedeutet, hier wäre es auf jeden Fall notwendig, bundesseitig finanzielle Unterstützung zu leisten, aber wir befürworten, wie gesagt, auf freiwilliger Basis Unterstützungsangebote auch für Betreiber von Anlagen mit kleineren Werten. Vielen Dank.

SV **Mathias Böswetter** (BDEW): Vielen Dank für die Frage, Herr Abgeordneter. Viel Wichtiges ist schon gesagt worden, ich möchte ergänzend zwei Risiken darstellen und dann noch einmal eine mögliche Lösung. Zunächst das erste Risiko, ich hatte es schon im Eingangsstatement genannt: Das KRITIS-Dachgesetz hat ja eigentlich – so wie es die letzten Jahre immer verhandelt und auch mit den Verbänden und den Branchen besprochen wurde – das Ziel gehabt, dort aufzubauen, wo man bei den kritischen Infrastrukturen schon Erfahrungen gesammelt hat. Da spielte ein Schwellenwert, der Regelschwellenwert von 500 000 eine ganz klare Rolle. Auch ist wichtig für die, die nicht unter den Schwellenwert fallen, die sind in der Erwartung in dieses KRITIS-Dachgesetz hineingegangen, dass sie *nicht* betroffen sein werden. Viele, die jetzt durch den niedrigen Regelschwellenwert in Zukunft vielleicht doch betroffen sein werden, haben die Erfahrungen aus der NIS-1-Umsetzung nicht, kennen nicht die Management-Systeme, die Prozesse, die damit einhergehen, müssen das noch lernen und ich glaube, das wird zu einer erheblichen Überforderung führen.

Das zweite Risiko, es ist hier schon angeklungen: Der Erfüllungsaufwand des Gesetzes war ja zumindest in der letzten Fassung vor einem Jahr, also noch vor Koalitionsbruch, „Pi mal Daumen“ angegeben. Da sprach der Regierungsentwurf von einmalig 1,7 Milliarden Euro und dann eben noch einmal jährlich 500 Millionen Euro. Der Umsetzungsplan KRITIS (UP KRITIS) hatte Anfang des letzten Jahres eine Kostenabschätzung allein für den Sektor Energie, das heißt für die Branchen Gas und Strom abgegeben, wo wir jährlich bei über 635 Millionen Euro waren und einmalig bei ungefähr 920 Millionen Euro – also wirklich abweichend! Wenn wir jetzt den Regelschwellenwert so absenken, dann wird es deutlich teurer. Wir haben übrigens diese Abschätzung im UP KRITIS auf Grundlage der Prozesskosten vorgenommen, da ist noch kein einziger Zaun gebaut worden – billiger wird es also nicht. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Böswetter. Es geht weiter mit der AfD-Fraktion, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank, Herr Vorsitzender. Meine erste Frage geht an zwei Sachverständige. Zum einen an Herrn Prof. Dr. Gause und an Herrn Atug. Und zwar geht es darum: Sind Sie der Meinung, dass das Ziel, eine größtmögliche Kohärenz zwischen dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und dem KRITIS-Dachgesetz herzustellen, erreicht worden ist? Und wenn nein, wo sehen Sie bei den beiden Gesetzen die Notwendigkeit gesetzlicher Anpassungen? Herr Prof. Gause, Sie hatten ja vorhin gesagt, dass Sie den Gesetzentwurf als gut empfinden, aber insbesondere auch noch eine Vertiefung beim BBK sehen, dass Sie das weiter stärken wollen. Und Herr Atug, ich hatte mir Ihren Schriftsatz durchgelesen. Insbesondere im Punkt 6 sind Sie schon näher darauf eingegangen und haben es vorhin auch gesagt, dass Sie das eher kritisch sehen. Vielleicht können Sie darauf noch einmal eingehen. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Janich. Dann machen wir es wie genannt in der Reihenfolge. Herr Gause und dann Herr Atug, bitte.

SV **Prof. Dr. Clemens Gause** (VfS): Jedes Gesetz ist irgendwo immer nur eine Anpassung an die gesellschaftlichen Rahmenbedingungen. Natürlich kann man immer daran kritisieren, aber wir haben keine Zeit. Und daher, würde ich sagen, kann man viele Dinge auch noch im Nachgang per Verordnung regeln. Grundsätzlich ist es so, wenn ich aus der Normierungs- und Standard-Ebene auf die konkrete Prüfung von Unternehmen gucke, dann gibt es natürlich den BSI-Standard, den man prüfen kann. Darin sind auch physische Elemente bereits enthalten. Insofern ist das, was der physische Schutz dann über die weiteren Normierungen und Standards nach anerkannten Regeln der Technik propagiert, bereits vorhanden, weil natürlich auch, und das haben die Vorredner ja auch gesagt, bereits in vielen Unternehmen und vielen Kommunen sehr viel Licht ist, aber auch noch Schatten. Und da ist es wichtig, dass diese Schattenthemen jetzt bearbeitet werden und eben physischer Schutz nachgearbeitet wird.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Atug.

SV **Manuel Atug** (AG KRITIS): Die wesentlichen Defizite sind genannt worden. Es sind die Definition der KRITIS-Sektoren, die lückenhaft oder gar nicht vorhanden sind, die Ausnahmeregelung dazu, die Schwellenwerte, die Versorgungssicherheit, die nicht adressiert ist und auch das Melderegime. Das heißt, wer kritische Versorgungsleistungen erbringt, muss halt in Resilienz investieren. Ansonsten steht jedem frei, stattdessen gern auch Plüschtiere herzustellen. Irgendwie müssen wir die Resilienz bekommen und die kostet nun einmal Geld. Man kann keine 100 Prozent Sicherheit bekommen, aber irgendwie gar nichts tun ist noch weniger als ein bisschen – man muss nicht immer die 100 Prozent erreichen. Das sehen wir auch bei der NIS-2-Umsetzung. Bei der NIS-1-Umsetzung in der Cybersicherheit wird seit 2015 BCM gefordert, das hat also jetzt zehnjähriges Jubiläum gehabt. 65 Prozent der KRITIS-Unternehmen haben ein BCM, was dem Anspruch des Gesetzes genügt; heißt im Umkehrschluss, dass 45 Prozent nach zehn Jahren Umsetzungsdefizit vielleicht auch Plüschtiere verkaufen sollten.

Kommunen können nur das leisten, was verpflichtend vorgesehen wird. Freiwillige Optionen bei 30 Milliarden Defizit – waren es, glaube ich, jetzt in diesem Jahr – sind dann nicht realisierbar. Das leuchtet auch uns als Zivilbevölkerung ein. Die müssen also a) verpflichtet, aber auch b) gefördert werden, wenn wir Resilienz in Deutschland haben wollen. Und diese ganzen Defizite, die wir haben, sind keine Kohärenz, die sind auch keine Resilienz, die sind auch keine Versorgungssicherheit, sondern ganz große Defizite, die wir haben und die bleiben auch so lange, wie wir das nicht ins Gesetz integriert bekommen!

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Es geht weiter mit der SPD-Fraktion. Frau Nasr.

Abg. **Rasha Nasr** (SPD): Vielen Dank, Herr Vorsitzender. Ich hätte eine Frage, die ich gern an Herrn Dr. Harrer und Herrn Stuffrein richten möchte. Es geht um den Regelschwellenwert. Der vorliegende Gesetzentwurf, der sieht einen Regelschwellenwert von 500 000 versorgten Einwohnern vor, die eine KRITIS-Anlage überschreiten muss, um den Regelungen des KRITIS-Dachgesetzes zu unterliegen. Das würde für mein Heimatland Sachsen bedeuten, dass Dresden und Leipzig darunterfallen, der Rest nicht. Herr Dr. Harre und Herr Stuffrein, wie bewerten Sie die Höhe des im Gesetzentwurf vorgesehenen Regelschwellenwertes von 500 000 zu versorgenden Einwohnern und welche Auswirkungen hätte dies auf die Resilienz unserer KRITIS? Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Frau Kollegin. Die Fragen sind an Herrn Harrer und an Herrn Stuffrein gerichtet. Bitte schön, Herr Harrer.

SV **Dr. Jürgen Harrer** (CISS): Vielen Dank für diese Frage. Ich beziehe mich letztendlich wieder auf meine Ausführungen von vorhin und sage: Der Regelschwellenwert von 500 000, der bekannt ist, der führt ja jetzt schon dazu, dass sich die Welt in zwei Teile teilt. Diejenigen, die ganz sicher über dem Regelschwellenwert liegen und etwas tun müssen und diejenigen, die sicher drunter liegen oder hoffen, darunter zu kommen, indem sie sich umgliedern. Resilienz erreichen wir nicht dadurch, dass wir hohe Schwellenwerte haben, sondern dadurch, dass sich möglichst viele beteiligen. Das ist einfach das Thema. Und ich habe bereits dargestellt: Im Gesetz stehen auch weitere Kriterien, die sogar in einer unterschiedlichen Gewichtung Einfluss in die Festlegung von dem, was hinterher zu

tun ist, finden können. Und ich glaube, es wäre sehr sinnvoll, eher in Richtung einer differenzierteren Betrachtung zu gehen als bei den 500 000 stehen zu bleiben, was in vielen Fällen einfach nicht passt. Sehr hilfreich sind dazu auch die Erläuterungen weiter hinten in dem Dokument, was mir zeigt, dass sich die Autoren des Gesetzentwurfes durchaus im Klaren drüber sind, dass man mit den 500 000 als Schwellenwert nicht glücklich wird.

SV **Christian Stuffrein** (DLT): Vielen Dank für die Frage. Der Schwellenwert von 500 000 versorgten Einwohnern basiert auf einer vom Bund getroffenen Annahme, dass diese Personenzahl bei einem Ausfall einer KRITIS mit Mitteln des Katastrophenschutzes versorgt werden kann. Das wurde empirisch aber nicht bewiesen. Letztlich bleibt dann also die Aufgabe vor Ort hängen und die örtlichen Behörden müssen schauen, wie sie damit umgehen und klarkommen. Ergänzend räumt der Gesetzentwurf die Möglichkeit ein, dass auch Abweichungen vom Regelschwellenwert vorgenommen werden können, wenn es im Einzelfall sinnvoll ist. Da sind wir beispielsweise die Rettungsleitstellen, die häufig auch in kommunaler Trägerschaft liegen. Nichtsdestotrotz zerfleddert natürlich der gesamte Regel-entwurf, wenn wir uns auf diverse Sonderfälle berufen. In Teilen sieht man das auch schon beim NIS-2-Umsetzungsgesetz. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Es geht weiter mit der Fraktion BÜNDNIS 90/DIE GRÜNEN, Herr Dr. von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Herr Vorsitzender, vielen Dank. Vielen Dank für Ihre Statements. Und es ist völlig unabweisbar, Herr Dr. Gause hat völlig recht – wir haben keine Zeit mehr zu warten. Trotzdem ist es bemerkenswert, und ich kann es uns allen nicht ersparen, gerade, weil man so lange gewartet hat, wenn jetzt ein Harmonisierungsgesetz diese Harmonisierung nicht leistet, dann ist das dramatisch in meinen Augen. Und ich finde das unterirdisch, auch schon, weil wir versucht haben, sozusagen mit der Restampel noch, mit der Union zu sprechen, das vor einem Jahr noch zu machen, da ist man schnöde davongeschickt worden und jetzt liefert man hier so ein Stückwerk ab. Der „Honkhase“ Herr Atug und Frau Petretto und Herr Dr. Kipker und viele andere haben es gesagt. Und jetzt würde ich es gerne noch einmal genauer erläutert bekommen haben, vielleicht von Frau Petretto aus der Sicht der Mitglieder ihres Verbandes, was es eigentlich bedeutet, wenn man keine Harmonisierung hat, keine einheitlichen Definitionen und Anforderungen. Und vielleicht kann Herr Dr. Kipker das dann aus wissenschaftlicher Sicht auch noch beschreiben. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kollege, so machen wir das. Frau Petretto zuerst und dann Herr Kipker.

SVe **Kerstin Petretto** (BDI): Vielen Dank, Herr Dr. von Notz. Was bedeutet das für die Unternehmen aus allen Branchen? Nun ja, die Herausforderung ist natürlich, dass wir zwei Bereiche haben. Wir sehen digitale und physische Sicherheit immer noch getrennt, obwohl wir in der hybriden Bedrohungslage, in der wir uns befinden, sehen – Herr Selen vom Verfassungsschutz nennt das eine „Entgrenzung der Bedrohungen“, die wir haben –, dass die Bedrohungen entgrenzt, miteinander verzahnt sind, physisch und digital. Wenn wir natürlich zwei gesetzlich getrennte Regelungen haben, dann müssen in den Unternehmen auch diese Bedrohungen, diese Angriffe, die sozusagen täglich auf sie einprasseln, letztlich auch getrennt voneinander präventiv bearbeitet werden, also Schutzmaßnahmen hochgefahren werden und dann im Meldefall muss man eben auch schauen, wie man reagiert. Das ist eine Komplikation, die da dann entsteht, die es eigentlich nicht gebraucht hätte, da gebe ich Ihnen recht. Aber wir sind nun einmal so weit gekommen, es hat eine ganze Legislaturperiode gebraucht, bis die Entwürfe entstanden sind. Bei NIS-2 sogar länger, das baut ja auf längeren Verfahren auf. Wir sagen eben, wir müssen jetzt damit arbeiten; wir können in den Rechtsverordnungen tatsächlich noch nachjustieren. Wenn wir jetzt noch einmal vier Jahre am KRITIS-Dachgesetz arbeiten, dann besteht weiterhin eine Rechtsunsicherheit, mit der niemandem geholfen ist! Die Unternehmen sagen, wir wollen ja was machen, wir machen ja auch schon was. Wenn wir aber nicht wissen, was der Staat von uns fordert, dann können wir das auch ganz schwer in die Vorstandsebenen hineinbringen und sagen, wir müssen in Schutzmaßnahmen investieren. Das heißt, wir brauchen auch eine bestimmte Vorgabe, ein bestimmtes Dach. Und deshalb sagen wir, die Einwendung ist wichtig, jetzt im fortlaufenden Prozess, um das entsprechend der Praxis so gut zu harmonisieren, wie es eben nötig ist, tatsächlich. Etwas anderes bleibt uns zum aktuellen Zeitpunkt, glaube ich, nicht übrig. Leider.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Kipker, bitte.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank auch für diese Frage. Man muss sich natürlich fragen, was bedeutet an der Stelle Kohärenz und Zusammenarbeit? Wir sehen es ja, viele Betreiber kritischer Infrastruktur fallen gleichzeitig unter die CER-Richtlinie und NIS-2. Wenn man beide Weltneben getrennt reguliert, haben wir doppelte Strukturen, unterschiedliche Melde- und Nachweispflichten in dem Bereich und natürlich zusätzlichen Verwaltungsaufwand – das sind genau die Ressourcen, die eigentlich in Sicherheit fließen sollen. Wir reden über limitierte Ressourcen und ein wirklich integriertes Dachgesetz, das würde einheitliche Begriffe angepasst an NIS-2/CER verwenden, Schwellenwerte und Sektoren vorgeben, ein gemeinsames Risiko- und Meldekonzept etablieren, das haben wir auch noch nicht, und eben auch viel, viel präziser abgestimmte Pflichten für Management und Betreiber festlegen, sodass wir wirklich diesen All-Gefahren-Ansatz haben. Weil wir nicht über Cybersicherheit oder analoge Bedrohung reden, sondern über *hybride* Bedrohung, das ist der Begriff. Wir brauchen einfach weniger Bürokratie für die Unternehmen, mehr Klarheit.

Auch für den Staat hätte das durchaus Vorteile. Wir hätten eine viel, viel bessere strategische Gesamtperspektive auf die KRITIS. Wir hätten bessere Lagebilder zu hybriden Bedrohungen – auch etwas, was von der Präsidentin des BSI Claudia Plattner schon seit längerem gefordert wird – und eben damit eine realistische Chance, unsere Resilienz tatsächlich zu erhöhen. Seitens der Betreiber haben wir auch zurzeit vielfach die Debatte: Bin ich überhaupt betroffen? Das sehen wir insbesondere bei NIS-2. Kohärenz würde unter dem Gesichtspunkt auch bedeuten, dass ein Betreiber eindeutig weiß, ob er betroffen ist, welche Pflichten gelten und welche Behörde zuständig ist. Und das schließt am Ende aus, dass wir Risiken zweimal managen, wie es teilweise jetzt noch der Fall ist, dass für denselben Sachverhalt unterschiedliche Behörden zuständig sind, unterschiedliche Nachweise in Teilen erbracht werden müssen, wir teilweise widersprüchliche Vorgaben zwischen NIS-2 und dem KRITIS-Dachgesetz haben. Und man sollte sich einmal überlegen: Wir haben immer noch das Thema Zwei-Klassen-Sicherheit und das ist natürlich besonders stark. Wir haben staatliche Einrichtungen, die für die Funktionsfähigkeit des Gemeinwesens mindestens genauso kritisch sind, die aber derzeit weitestgehend außenvor bleiben, wie auch meine Vorrednerinnen und Vorredner angemerkt haben. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Und es geht weiter mit Die Linke, Herr Köstering.

Abg. **Jan Köstering** (Die Linke): Vielen Dank, Herr Vorsitzender. Herr Atug, Sie kritisierten in Ihrer Stellungnahme, dass die Einrichtungen des Bundes, also die meisten Ministerien, Behörden und öffentlich-rechtlichen Einrichtungen vom KRITIS-Dachgesetz ausgenommen sein sollen. Können Sie das einmal anhand eines konkreten Beispiels ausdrücken, was das für Einrichtungen sein könnten und was deren Ausfall zur Folge hätten? Und daran anschließend die Frage, ob das KRITIS-Dachgesetz an dieser Stelle ausreichend auf das NIS-2-Umsetzungsgesetz abgestimmt ist. Also gibt es da dieselben Ausnahmen oder könnte man der Ansicht sein, dass bei Einrichtungen des Bundes ohnehin nur Fragen der IT-Sicherheit berührt werden und daher im KRITIS-Dachgesetz auch nicht geregelt werden müssen, weil sie im BSI-Gesetz ohnehin geregelt sind?

Und das ist heute auch schon mehrfach angesprochen worden: Der Bundesrat hat in seiner Stellungnahme kritisiert, dass kritische Anlagen erst unter die Regulierung fallen, wenn der Ausfall mindestens eine halbe Million Menschen treffen würde. Der Bundesrat schlägt, auch das ist erwähnt worden vor, die Schwelle auf 150 000 Menschen abzusenken. Sind solche Schwellenwerte aus Ihrer Sicht überhaupt ein probates Mittel, die Normadressaten dieses Gesetzes zu bestimmen? Und welche Alternativen wären denkbar?

Amt. Vors. **Josef Oster** (CDU/CSU): Ich würde gern zur Beantwortung kommen. Herr Atug, das waren jetzt drei Fragen. Es bleibt aber bei vier Minuten zur Beantwortung.

SV **Manuel Atug** (AG KRITIS): Na gut, dann versuche ich das. Einrichtungen des Bundes, wenn man sich das am Bundesverwaltungsamt oder am BSI selbst einfach einmal anguckt; reden wir gar nicht von Cyber- oder von Hybridbedrohungen oder so etwas, reden wir einfach einmal von einem Naturereignis wie im Ahrtal: Die Deutsche Bahn hat vor zwei, drei Wochen alle 13 Bahnhofstationen wieder

vollständig in Betrieb nehmen können. Die „Ahrtal-Bahn“ ist aber immer noch nicht vollständig betriebsfähig. Das ist vier Jahre her! Und wenn wir das beim Bundesverwaltungsamt haben, dann läuft einfach gar nichts mehr im Bundesbetrieb. Dann ist wirklich Stillstand. Und das ist einfach im Hintergrund das Back-Office, was dann nichts mehr tun kann. Die Betreiber von kritischer Infrastruktur oder die Bevölkerung können dann gern einmal versuchen, ein Amtshilfeverfahren einzuleiten oder Hilfestellung zu bieten. Da geht niemand ran, weil das Gebäude nicht mehr steht. 13 Bahnhöfe waren einfach nicht mehr existent. Tonnen von Erde waren nicht mehr da, worauf die Schienen lagen. Das heißt, dort müssen Tonnen von Erde jahrelang angekarrt werden, um überhaupt wieder Schienen legen zu können. Und solche Zustände können wir durch die Gefahren, die im KRITIS-Dachgesetz eigentlich adressiert werden, verhindern. Oder wir machen aus diesen Naturereignissen Naturkatastrophen, denn wir haben nicht die richtigen Maßnahmen gewählt. Genau das sind die Szenarien, die wir an solch einer Stelle haben können, wenn wir beim Bundesverwaltungsamt oder beim BSI oder jeder anderen Einrichtung des Bundes meinen, dass die da nicht darunterfallen oder das nicht müssen. Dasselbe gilt für Landräte, für Kommunen und andere. Die Bevölkerung hat nichts davon, wenn sie weggecybert wurde oder weggespült wurde. Sie hat ein Defizit, und zwar ein richtig heftiges.

Die Ausnahmen? Also wir haben grundsätzlich ein Problem mit Ausnahmen. Ausnahmen bedeuten ja immer: Mach das mal nicht! Und wenn wir von diesen Katastrophenszenarien reden und nicht von kleinen Störfällen oder hier fallen einmal ein paar Bit-Werte um, sondern wir reden von physischen existenziellen Bedrohungen, dann ist es wirklich so, dass jede Ausnahme eigentlich bedeutet: Wir bedrohen aktiv die Bevölkerung durch Unterlassung von Hilfe.

Die Schwellensenkung auf 150 000 Menschen, ob das sinnvoll ist? Nein, denn es ist genauso sinnvoll, wie die Zahl 500 000 aus der Luft zu greifen und zu sagen, das ist jetzt der Maßstab. Was wir brauchen, ist eine wirkliche wissenschaftliche Evaluierung. Und zwar pro Branche. Was ist eigentlich da der Maßstab, der hilft? Und wie kriegen wir den über die Jahre wirklich auf Null reduziert? Denn noch einmal, so wie im Eingangsstatement, ob ich in einem kleinen Dörfchen mit 10 000, 20 000, 50 000 Einwohnern lebe oder in einer Großstadt wie Köln oder Hamburg oder München: Muss ich jetzt wählen in der Form, dass ich sage, na ja, in den drei Großstädten wird mir geholfen, wenn ich Versorgungsprobleme und -defizite habe? In den kleinen Städten können die Leute dann einfach sterben? Oder wie sehen wir das? Also wählt man seinen Standort in Deutschland nicht mehr anhand der Daseinsvorsorgepflicht des Staates aus, sondern danach, wo der Staat vielleicht noch ein bisschen etwas hinkriegt? Und die Betreiber kritischer Infrastruktur wie auch die öffentlichen Betreiber sagen, na ja, wenn wir nicht gefreiwilligt werden, von nix kommt nix und dann machen wir auch nix. Wir haben ja auch in den diversen Statements gehört, wenn es nichts bzw. kein Geld gibt, dann kann man nichts umsetzen. Jeder hätte gern Geld. Wir würden gern mehr Versorgungssicherheit für die Bevölkerung haben. Insofern ist der wissenschaftlich evaluierte Ansatz der richtige, um das langfristig auf null zu bekommen. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Atug. Damit sind wir bei der ersten Fragerunde durch. Wir sind gut in der Zeit. Wir können uns mindestens eine vollständige weitere Runde leisten. Es geht weiter mit der CDU/CSU-Fraktion und das Wort hat Herr Schmidt.

Abg. **Sebastian Schmidt** (CDU/CSU): Herr Vorsitzender, meine Damen und Herren. Eine Frage an Dr. Gause: Der Entwurf des KRITIS-Dachgesetzes sieht umfassende Resilienz-Maßnahmen in zehn Sektoren vor. Die in diesen Sektoren tätigen Unternehmen stehen vor großen Herausforderungen, da sie die hohen organisatorischen, technischen und finanziellen Anforderungen umzusetzen haben. Wie bewerten Sie vor diesem Hintergrund die bisherigen Anstrengungen der betroffenen Sektoren, der Unternehmen, im Hinblick auch auf die Umsetzung der Resilienz-Maßnahmen und welche Voraussetzungen sind notwendig, damit insbesondere kleine und mittlere Unternehmen mit großem Erfüllungsaufwand diese Anforderungen erfolgreich und auch nachhaltig erfüllen können? Und eine zweite Frage möchte ich anschließen an Frau Petretto. In § 13 schafft das KRITIS-Dachgesetz viele Rechtsgrundlagen für den Ausbau von Resilienz-Maßnahmen auf Seiten des Betreibers. Dabei stehen bauliche und technische Maßnahmen im Fokus, aber auch personelle Maßnahmen. Haben die Betreiber aus Ihrer Sicht damit ausreichende Spielräume, um sich

gegen Risiken abzusichern, insbesondere auch Blick auf die Gefahr, die von Innentätern ausgeht? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kollege. Dann die Antworten in der genannten Reihenfolge, Herr Dr. Gause und dann Frau Petretto.

SV **Prof. Dr. Clemens Gause** (VfS): Vielen Dank für die Frage. Wie ich bereits sagte, ist natürlich in der Fläche und auch sektorübergreifend viel Licht und Schatten. Es gibt einige, die sind sehr weit mit dem Ausbau ihres physischen Schutzes und Schutzkonzepten. Die machen auch, wie es im Gesetz gefordert ist, entsprechende Risikoanalysen und so weiter, also eigentlich permanent, nicht nur in wenigen Monaten, sondern es ist jeden Morgen eine Lage. Da wird sich darauf verständigt, da bestehen auch ganz solide und belastbare Kommunikationsstrukturen, auch europaweit bereits schon, da wird Sicherheit gelebt. Aber es gibt auch Bereiche, die etwas dünner ausgestattet sind, um es vorsichtig zu formulieren. Wir hatten alle diese Fälle auch in der Presse. Stichwort „Mittelspannungsstromnetz“, wo schlichtweg Sensoren fehlen. Ein Sensor kostet 87,50 Euro. Den kann man anbringen. Dann weiß man, wenn da sich jemand an dem Mittelspannungs-Transformator zu schaffen macht. Wie gesagt, solche Aufschaltungen kann man machen. Es geht auch in einem kostenmäßig überschaubaren Rahmen in der Fläche. Es muss nicht immer nur der Zaun sein, sondern man kann heutzutage sehr viel auch anders überwachen.

Und der zweite Teil geht natürlich in die Richtung wirtschaftspolitische Maßnahmen. Ich meine, all diese Dinge sind in Teilen auch Hochtechnologie, sind in Teilen aber auch solides Bauwesen. Und es wäre eine große Freude zu sehen, wenn wir hier wirtschaftspolitische Maßnahmen anknüpfen. Ich sage einmal, der Automobilbranche geht es gerade schlecht. Da sind Ingenieure, Techniker, die man vielleicht auch für andere Bereichen nutzen kann. Ich würde mir wünschen, wenn wir hier in einen sicherheitstechnischen oder sicherheitswirtschaftlichen Boost kommen, hier einen Jobmotor kreieren, neue Jobformate entwickeln, neue Berufsbilder. Auch würde ich mir, und das sei mir bitte noch gestattet, wünschen, auch mehr Kollegen zu bekommen. Ich bin mit meinem Fachbereich für Sicherheitstechnik ein kleiner, seltener Schmetterling und es wäre mir eine große Freude, wenn ich noch ein paar mehr dazu bekommen würde. Ende.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Dr. Gause. Frau Petretto, bitte.

SVe **Kerstin Petretto** (BDI): Vielen Dank. Die Frage war, ob die Unternehmen genügend Möglichkeiten, genügend Optionen an der Hand haben, um Mitarbeitende prüfen zu können in Bezug auf das Risiko der Innentäterschaft. Wir haben festgestellt: nein, haben sie nicht in vielen Bereichen. Es gibt Ausnahmen, beispielsweise im Bereich der Luftsicherheit, Flughafensicherheit, aber in den meisten KRITIS-Sektoren haben Unternehmen heute keinen rechtssicheren Rahmen, um Personen in sicherheitssensiblen Funktionen durch staatliche Sicherheitsbehörden prüfen zu lassen. Die können natürlich private Anbieter beauftragen, aber die schauen sich dann eben das Führungszeugnis an, aber viel mehr können sie nicht machen. Das müssen nicht die Leute sein, die wirklich einen Schutzauftrag haben. Das kann auch, um ein Beispiel zu nennen, die Assistentin sein, die Zugriff auf sämtliche sicherheitssensible Bereiche hat. Man hat aktuell keine Chance, eine Sicherheitsüberprüfung zu bekommen. Das heißt, hier haben wir einen Vorschlag einer freiwilligen Vertrauenswürdigkeitsüberprüfung erarbeitet, die Unternehmen beantragen können. Und dann können sie es genau überprüfen, wo die Risikobewertung es aus ihrer Sicht erfordert, und zwar für Personen in hochsensiblen Bereichen. Diese Option ist auch ausdrücklich in Artikel 14 der CER-Richtlinie vorgesehen und ergänzt auch noch die Sicherheitsanforderungen der NIS-2-Richtlinie, die nämlich unter anderem Schulungs- und Sensibilisierungsmaßnahmen für das Personal als Bestandteil des gesamten Risikomanagements vorsieht, aber eben auch aktuell noch keine rechtliche Grundlage schafft, damit Unternehmen das tatsächlich umsetzen können. Und deshalb plädieren wir sehr stark hier für eine Einarbeitung dieser Möglichkeit, am besten ins Gesetz, im Notfall auch hier wieder in die Rechtsverordnung, aber besser, und das hatten wir auch mit dem BMI öfters besprochen, wäre es gewesen, das in die Gesetze zu NIS-2 und KRITIS hineinzubringen. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Ich danke Ihnen und es geht in der Fraktionsrunde weiter mit der AfD, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank, Herr Vorsitzender. Ich habe zwei Fragen an zwei Sachverständige. Die erste Frage geht an Herrn Dr. Harrer und

die zweite an Herrn Böswetter. Herr Dr. Harrer hatte in seinem Eingangsstatement gesagt, dass es Infrastrukturen gibt, die man nicht schützen kann. Mir ist klar, die Ostsee ist groß und damit bestimmt ein solcher Bereich. Vielleicht können Sie einmal auf so wesentliche Sachen eingehen, worauf wir vielleicht unser Augenmerk noch einmal legen können. Herr Prof. Dr. Gause hat ja gerade gesagt, Sensorik in der Mittelspannung könnte zum Beispiel eine Lösung bei so etwas sein. Haben Sie vielleicht Ideen, wo man in diesen Bereichen, wo es jetzt noch schwierig ist, vielleicht zukünftig gesetzliche Vorbereitung schaffen kann, dass das in dieser Richtung in der Praxis umgesetzt werden kann?

Meine Frage an Herrn Böswetter als Verbandsvertreter: Sind die Betreiber von KRITIS aus Ihrer Sicht praktisch darauf vorbereitet, sämtliche Risikobewertungen in allen Sektoren durchführen zu lassen und geeignete Resilienz-Pläne zu erstellen? Wie sieht es in der Praxis bei Ihren Mitgliedern aus? Das würde mich interessieren. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Kollege. Dann bitte zur Beantwortung. Erst Herr Dr. Harrer und dann Herr Böswetter.

SV **Dr. Jürgen Harrer** (CISS): Vielen Dank für diese Frage. Infrastrukturen, die man nicht schützen kann, also beispielsweise Eisenbahnschienen, Autobahnen, Hochspannungsleitungen, Tiefseekabel, bei denen klappt das nicht mehr, was man so als übliche Logik hat. Wenn es im Vergleich dazu um ein Rechenzentrum in einer Großstadt geht, dort kann ich eine Rundum-Sicherung machen, ich kann also verhindern, dass sich Leute auf die Anlage zubewegen, ich habe einige Möglichkeiten der Prävention. Wenn es doch jemand versucht, dann habe ich die Möglichkeit einer Detektion. Ich erkenne, dass da etwas passiert. Idealerweise habe ich die Möglichkeit einer Intervention. Ich kann nach der Alarmierung jemanden hinschicken, die Polizei hinschicken, um zu verhindern, dass eine begonnene Straftat vollendet wird und brauche dann, wenn doch was kaputt gegangen ist, die Möglichkeit zur Stabilisierung, also ich muss in irgendeiner Form damit umgehen, den Notbetrieb einleiten.

Wenn ich die Infrastrukturen habe, die ich nicht schützen kann, wie beispielsweise die Hochspannungsleitungen, da fällt die Prävention weg. Ich kann es nicht einzäunen. Die Detektion ist möglich, ich kann mit Sensoren arbeiten. Die Intervention scheidet meistens auch aus. Das heißt, die sind zu weit weg, zu disloziert, als dass da kurzfristig Einsatzkräfte da sein können, um zu verhindern, dass ein Ereignis, was begonnen wurde, gestoppt wird, bevor es vollendet werden kann. Umso wichtiger wird das Thema der Stabilisierung. Deswegen mein Plädoyer für Redundanzen, Reserven und die Fähigkeit zur Schnellinstandsetzung. All das gab es früher auch in den großen Unternehmen, wurde aber aus Effizienzgründen herausgekürzt, weil die Balance zwischen Effizienz und Resilienz ein Stück weit verloren gegangen ist.

SV **Mathias Böswetter** (BDEW): Vielen Dank für Ihre Frage, Herr Abgeordneter. Ein Großteil unserer Mitgliedsunternehmen ist im Rahmen der NIS-1-Umsetzung auch in der Einführung von Informationssicherheitsmanagementsystemen mit entsprechenden Risikoanalysen schon vertraut. Was sich jetzt auch im Sinne des All-Gefahren-Ansatzes durch NIS-2, aber eben auch durch die CER-Richtlinien-Umsetzung ergeben wird, also mit dem KRITIS-Dachgesetz, hängt auch maßgeblich davon ab, wie die nationalen Risikoanalysen gewissermaßen die „Großrisikowetterlage“ bestimmen und auf deren Grundlage werden dann auch die Unternehmen ihre Risikoanalysen entsprechend dem KRITIS-Dachgesetz umsetzen. Ich glaube, da sind sie, wie ich schon gesagt habe, gut aufgestellt. Sie kennen eben im großen Teil diese Risikomaßnahmen. Sie kennen die Handwerksmittel der Risikoanalysen und werden auch dort, glaube ich, gut aufgestellt sein. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön, Herr Böswetter. Wir fahren in der Fraktionsrunde fort. Die SPD, Herr Baldy, hat das Wort.

Abg. **Daniel Baldy** (SPD): Vielen Dank, Herr Vorsitzender. Ich habe zwei Fragen an zwei Sachverständige. Die erste geht an Frau Borcherding: Sie haben eingangs gesagt, das Meldewesen darf keine Einbahnstraße sein, sondern Sie erwarten im Gegenzug auch Meldungen. Ich gehe einmal davon aus, Sie wollen jetzt nicht einen – oder vielleicht wollen Sie das doch – täglichen Newsletter? Kurzum, wie stellen Sie sich denn das Meldewesen vor? Nicht das, was Sie abgeben, sondern das Meldewesen, oder die Meldungen, die Sie empfangen.

Und die zweite Frage an Herrn Dr. Harrer: Das Thema Drohnen, Drohnensichtungen ist ja in letzter Zeit immer häufiger und auch in der Presse. Es gab

einzelne Stellungnahmen, die gesagt haben, das Thema Drohnen wird im Gesetzesentwurf gar nicht so angefasst, wie es das sollte. Können Sie zu dem gesamten Themenkomplex einmal Stellung beziehen? Umfasst der Gesetzentwurf auch das Thema Drohnenabwehr? Und insbesondere: Können Unternehmen oder kritische Infrastruktur das eben auch leisten, zumindest die Detektion dann eben auch adäquat umzusetzen?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fangen an mit Frau Borcherding, und dann geht es mit Herrn Dr. Harrer weiter.

SVe **Sylvia Borcherding** (50Hertz): Vielen Dank für die Frage. Meldewesen bedeutet für uns, dass wir Stand heute einseitig aufgefordert sind, Informationen, Interventionen, Besonderheiten zu melden. Und in Zukunft wird das noch intensiviert werden mit der großen Unsicherheit, dass wir zum einen nicht wissen, wie relevant eigentlich diese Information für eine Gesamtgemengelage und für ein Gesamtlagebild ist. Also sind das Vorfälle, die auch an anderer Stelle vorgekommen sind und lässt sich daraus etwas für eine Bedrohungslage ableiten oder nicht? Das ist der erste Aspekt. Also wenn an verschiedenen Stellen in Deutschland aus Masten Material geklaut wird, und es kommt nur an einer Polizeistation an, dann lässt sich daraus nicht unmittelbar ableiten, dass vielleicht überprüft wird, inwiefern dieses Material brennbar ist oder inwiefern es gebogen werden kann. Habe ich aber zehn dieser Meldungen, dann müssen wir anders darauf reagieren – im Übrigen auch bundesweit anders darauf reagieren. Im Moment bekommen wir sehr häufig die Rückmeldung, dass aus Datenschutzgründen diese Informationen auf dem Zweimeldekommunikationsweg nicht geteilt werden können. Wir brauchen diese Informationen aber sehr dringend, um uns auf mögliche Interventionen vorzubereiten. Das heißt zum Beispiel Mitarbeitende in Bereitschaft zu versetzen. Wenn wir wissen, dass es eine zunehmende Gefährdungssituation in einer bestimmten geografischen Region gibt, dann werden unsere Mitarbeitenden in eine Bereitschaft versetzt und sind in der Lage, sehr kurzfristig zu reagieren. Wenn wir diese Informationen nicht haben, ist es nicht möglich. Und nein, wir wollen natürlich nicht jeden Tag einen Newsletter. Wir sind auch sehr dafür, dass diese Informationen nur in vertraulichen Kreisen geteilt werden. Das müssen Sie aber in Zukunft bitte.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank.

SV **Dr. Jürgen Harrer** (CISS): Vielen Dank für die Frage. Das Thema Drohnen. Ich denke, da haben wir in Deutschland allgemein grundsätzlich Nachholbedarf. Das sind wir in Anbetracht der aktuellen hybriden Bedrohungen weder in Bezug auf die Detektion noch auf die Intervention an der Stelle, an der wir sein sollten. Im Gesetz kommt es natürlich kurz. Und die Frage, was ein Betreiber leisten kann, möchte ich einmal in der Richtung beantworten: Wenn Drohnen eingesetzt werden, dann zur Spionage, also natürlich zur Verunsicherung der Bevölkerung, um den Flugbetrieb lahmzulegen, aber ansonsten aus Gründen der Spionage oder aus Gründen der Sabotage. Und zum Thema Spionage und Sabotage haben viele Unternehmen in der Vergangenheit schon Maßnahmen ergriffen. Die gehen zum Beispiel her und verlagern die Räume, in denen kritische Besprechungen sattfinden sollen, nach innen ins Gebäude hinein, weg von der Außenwand. Ansonsten werden entsprechende Abschirmungsmaßnahmen, elektronische Störmaßnahmen erforderlich. Und wenn es um das Thema Sabotage geht, da verschließen Unternehmen schon seit Jahren Gebäudeeröffnungen im Außenbereich für Heizung, Klimaanlage oder Luft, die oben am Dach sind, mit Sperrgittern, um zu verhindern, dass Mini-Drohnen einfliegen oder etwas abwerfen können. Diese Möglichkeiten werden schon ergriffen, aber eben von den Unternehmen, wie es Dr. Gause dargestellt hat, die schon seit Jahren aware sind und vieles tun. Das werden wahrscheinlich die meisten Global Player aus Deutschland sein, die schon längst Sicherheitsmaßnahmen, Schutzmaßnahmen, Resilienz-Maßnahmen ergriffen haben, die weit über das hinausgehen, was das Gesetz mit sich bringt, auch im Bereich der Drohnen ganz vorn dran sind und dann in Bezug auf die Anforderungen aus dem KRITIS-Dachgesetz eher mit den Schultern zucken und sagen: Okay, machen wir eh. Wichtig wird es sein, im Rollout an viele andere zu gehen. Da ist tatsächlich das Thema weniger ein juristisches, meine ich, sondern eines, was die Fähigkeiten angeht, der Detektion und eines Lagebildes und der Intervention, was man damit macht, weil das Abschießen der Drohnen im zivilen Bereich offensichtlich nicht die Lösung ist. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Es geht weiter mit BÜNDNIS 90/DIE GRÜNEN, Herr Dr. von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Genau. Ich fange vielleicht einmal damit an, dass ich glaube, dass wir dramatisch schlecht aufgestellt sind. Weil gerade im Bereich der Energieversorgung gesagt wurde, so schlimm ist es nicht oder es zumindest so zu verstehen war: In meiner Wahrnehmung gibt es praktisch jeden Tag in Deutschland Zutritte auf kritische Infrastruktur bei der Energieversorgung. Es wird systematisch ausspioniert, wo was ist, es wird fotografiert, kartografiert und so weiter. Und Frau Borcherding, weil sie es ansprechen: Ich hoffe, die Unternehmen melden das alle und irgendwo laufen die Informationen in diesem Land hoffentlich zusammen. Aber sie kriegen sie ja nicht. Insofern weiß niemand, wo gerade Leute unterwegs sind, die das machen. Das ist ein untragbarer Zustand! Und weil es vorhin angesprochen wurde: Die Präsidenten waren wirklich vollkommen klar im Hinblick auf den Zuwachs und die Eskalationsfähigkeit dieser Themen in den nächsten Monaten. Der BND-Präsident hat gesagt, er gehe von einem Angriff Russlands vor 2029 aus! Das kann ja jeder einmal deuten, was das in der Dramatik der Dinge, die wir hier besprechen, heißt. Denn das hängt miteinander zusammen, das Ausspionieren von Infrastruktur und die Potenzialität von Angriffen auf die Infrastruktur, das ist unmittelbar miteinander verknüpft. Gut, sei es drum.

Noch einmal kurz an Frau Petretto und Herrn Dr. Kipker die Frage: Jetzt sind wir spät dran und müssen „in die Puschen kommen“, trotz aller Unzulänglichkeiten. Wir sind in einem parlamentarischen Verfahren. Was kann hier noch gerettet, gemacht werden? Was sind die Dinge, die wir hier noch so, wenn wir nicht grundsätzlich herangehen, aber jetzt hier im Verfahren machen können? Wo können wir Abhilfe schaffen? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Kollege. Dann bitte ich zunächst Frau Petretto und dann Herrn Dr. Kipker um Beantwortung dieser finalen Fragen.

SVe **Kerstin Petretto** (BDI): Vielen Dank, eine sehr große Frage zum Schluss. Ich habe drei Punkte genannt, von denen wir glauben, die müssen wirklich angegangen werden: Zum einen die Ausnahme des Staates aus dem Bereich des KRITIS-Dachgesetzes; also Staat, Verwaltung auf Bundes- und Landesebene müssen hier auch hinein, müssen auch reguliert werden, damit hier auch gehärtet werden kann – nicht nur im digitalen Bereich, sondern auch im physischen, das ist sehr wichtig!

Die Frage, die Basis von Sicherheitsvorkehrungen innerhalb von Unternehmen, glauben wir auch, muss tatsächlich hinein, deshalb noch einmal unser Vorschlag, dass man die freiwillige Vertrauenswürdigkeitsüberprüfung mit hineinnimmt. Und aus unserer Sicht muss die Vektor-Drohne auch adressiert werden. Wir haben den All-Gefahren-Ansatz, das heißt nur, dass alle verschiedenen Vektoren schon inkludiert sind. Aber hier klafft tatsächlich eine Rechtslücke, an die wir heranmüssen. Um schnell vorwärtszugehen, bleibt uns immer noch die Option der Rechtsverordnung. Ich sage das ungern, weil wir dafür sind, dass so viel wie möglich im Bundestag, im Parlament beschlossen wird und dass man sofort Rechtssicherheit hat, wenn das Gesetz durch ist und dass man da nichts nachlagert. Aber um schneller voranzukommen und vor allem um die Expertise aus der Praxis hineinzunehmen, müssen wir hier in vielen Bereichen den Weg über die Rechtsverordnung gehen, um Regelungen zu schaffen; aber da kann ich wirklich nur appellieren. Es ist ja auch angelegt, dass Verbände und Experten aus der Praxis in die Erarbeitung der verschiedenen Rechtsverordnungen einbezogen werden. Ich kann nur den Appell an Sie alle richten: Sehen Sie zu, dass das auch wirklich umgesetzt wird und eben nicht nur mittels Stellungnahmen im Sinne von, bitte meldet euch in fünf Tagen und schafft eine abgestimmte Position, sondern ermöglichen Sie wirklich ein Gespräch. Das ist tatsächlich essentiell. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Ja, danke. Herr Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank für diese Frage. Ich hatte es in meiner Stellungnahme schon ein bisschen angeführt: Es geht vor allem auch darum, Komplexität zu reduzieren – die haben wir wirklich noch massiv. Und gerade für die kleinen mittelständischen Unternehmen ist teilweise nicht die Zahl der Pflichten das Hauptproblem, sondern die Komplexität der behördlichen Landschaft. Ich spreche mich sehr dafür aus, für Betreiber eine zentrale Stelle als primären Ansprechpartner zu haben, vielleicht kombiniert mit einem einheitlichen digitalen Portal und dass dann die Informationen, die erst einmal extern an einer zentralisierten Stelle

gesammelt werden, intern innerhalb der Behörden und deren Verwaltung weiterverteilt bzw. in die richtigen Kanäle geschickt werden. Das ist aber etwas, was wir tatsächlich seit mehreren Jahren schon so besprechen. Für Mittelständler reden wir da über den Punkt Vertrauen. Vertrauen sehen wir bei der Cybersicherheit und wir sehen es beim physischen Infrastrukturschutz. Teilweise fehlt jedoch noch das Vertrauen, mit staatlichen Einrichtungen zusammenzuarbeiten, weil eben ein einheitliches Gesicht, eine einheitliche Ansprechstelle fehlt und teilweise, weil niedrigschwelliger, verständlicher Zugang zu Aufsichtsbehörden nicht vorhanden ist und natürlich auch, weil teilweise intensive Beratungs- und Unterstützungsangebote fehlen. Das wäre der erste Punkt, den ich als wichtig erachten würde.

Zum Zweiten: Resilienz-Pflichten klar strukturieren. Da kann man durchaus sagen, dass viel Luft nach oben ist, was Prävention, Vorbereitung, Bewältigung und Nachsorge von Krisenmaßnahmen also eine weitere Konkretisierung der Vorgaben angeht. Gleiches gilt für die realistische Ausgestaltung von Fris-ten. Ich glaube, das ist etwas, was wir definitiv angehen können. Wir haben teilweise wirklich überlange Übergangsfristen, das Inkrafttreten erst 2030 und so weiter, das hatte Manuel Atug ja auch schon angesprochen, steht in einem deutlichen Spannungsverhältnis zu der aktuell schon wahrgenommen massiven Bedrohungslage im Bereich KRITIS-Schutz.

Und last but not least wäre es natürlich auch schön, einfach die Unterstützungsfunktion des Staates noch stärker auszubauen, Muster, Leitfäden, Best-Practice-Sammlung, Standardschulungen, Übungen bereitzustellen und vielleicht das Ganze auch auf einer Plattform irgendwo zu zentralisieren und zugreifbar zu machen. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Und wir kommen zu den beiden Fragen der Fraktion Die Linke. Herr Köstering, bitte.

Abg. **Jan Köstering** (Die Linke): Vielen Dank, Herr Vorsitzender. Ich gelobe Besserung und habe zwei Fragen an Herrn Atug. Herr Atug, Sie haben in Ihrem Eingangsstatement schon Kritik an der Beteiligung von Wirtschaft, Wissenschaft und Zivilgesellschaft im Gesetzgebungsverfahren geübt. Bei der Umsetzung des Gesetzes sind es nur die Länder, die monieren, dass wesentliche Regelungen erst in Verordnungen getroffen werden sollen, die aber nicht zustimmungspflichtig im Bundesrat sein sollen. Jetzt jenseits der verfassungsrechtlichen Schwierigkeiten, die es da aus unserer Sicht gibt: Ist es auch hinsichtlich des Ziels des Gesetzes hilfreich, den Ländern da ohne ihre Einbindung Vorgaben zu machen? Sehen Sie auch an anderen Stellen des Entwurfs Probleme?

Und auch ich möchte zum Schluss mit meiner zweiten Frage dann noch auf das Thema Drohnen zu sprechen kommen. Da reicht die Bedrohungslage vom bloßen Ausspähen bis hin zu tatsächlichen Angriffen durch Kamikaze-Drohnen oder dem Abwurf von Sprengsätzen oder schmutzigen Bomben. Wie könnte dieses Thema aus Ihrer Sicht sinnvoll in die Regelungen eingepflegt werden? Oder ist hier ohnehin nicht ein gesamtstaatlicher Ansatz gefragt, also eine allgemeine Drohnenabwehr und nicht eine anlagenbezogene Drohnenabwehrstruktur? Oder sind Sie vielleicht auch der Meinung, dass man das gar nicht so gegeneinander diskutieren kann? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kollege. Herr Atug, bitte.

SV **Manuel Atug** (AG KRITIS): Was das Beteiligungsdefizit angeht: Ich meine, die Expertise ist vorhanden. Und wir hören auch von den Beteiligten aus der Wirtschaft oder von Verbänden, dass sie Geld fordern. Das ist sehr einfach und schnell gesagt – ansonsten, wenn man die Gelder nicht erzwingt oder bereitstellt, sagt man, dass dann an vielen Stellen nichts gemacht werden kann oder dass es zu teuer ist. Wenn dann gefragt wird, ob man gut aufgestellt sei, behauptet man ja. Aber wenn man gut aufgestellt ist, braucht man eigentlich kein Geld. Insofern haben wir ja beim Beteiligungsdefizit das Problem, dass zu wenig wissenschaftlicher, zivilgesellschaftlicher Expertenteil angehört und ein Gleichgewicht hineingebracht wird, denn die Betroffenen werden am Ende die Bevölkerung sein. Das darf man natürlich nicht nur auf den Kostenfaktor reduzieren. Wenn es sich darauf reduziert, dann muss man auch gemeinsam zusammensitzen und gemeinsam Lösungen finden. Also man kann nicht einfach den einen oder den anderen die Kosten auferlegen, da muss man schon Konsens finden und der muss dann ausgeglichen sein. Ich meine, am Ende hilft es nicht, wenn wir da den Ländern Vorgaben machen, dass theoretisch, unter Umständen ab 2030 irgendwas vielleicht irgendwie kommt und man in meiner Hochrech-

nung ja dann irgendwann so gegen 2035, 2040 vielleicht irgendetwas hat! Herr Dr. von Notz hat gerade schön dargestellt, dass die Angriffssituation vielleicht eher vor 2029 ist. Gut, wir haben also keine Zeit, noch weniger Zeit als vorher, wir eiern aber immer noch herum! Noch einmal: Das ist für uns dann Menschenleben-gefährdend und nicht mehr witzig! Also insofern würden wir uns sehr freuen, wenn diese Beteiligungsdefizite behoben und solche Aussagen zur Abwechslung auch einmal ernstgenommen werden. Oder man setzt sich vernünftig und konstruktiv zusammen und klärt das Ganze auch wirklich gemeinsam und diskutiert eben nicht einseitig. Wenn es also bei den Ländern und Kommunen nicht erzwungen wird, dann haben die halt kein Geld, um die freiwilligen Dinge zu tun, das leuchtet ja Jedem ein, also ich habe volles Verständnis dafür. Aber ich habe oder wir als AG Kritis haben eben kein Verständnis dafür, wenn wir stattdessen lieber Menschenleben bedrohen. Das ist irgendwie keine Beteiligungsstruktur, die wir wünschen.

Zu den Drohnen und der Bedrohungslage: Es ist ja so, dass wir in der Presse im Wesentlichen im Moment nur von ein paar Überflügen bei ein paar Flughäfen reden. Es ist natürlich deutlich mehr. Wir müssen die Detektion, Meldung und soweit möglich die Abwehr von Drohnen – und da reden wir als AG KRITIS von unbemannten Luftfahrt-, Land- und Wassersystemen, und zwar in der gesamten Sicherheitskette – adressieren. Das ist ein Defizit. Wir haben also nicht die gesamte Sicherheitskette von Prävention, Detektion, Alarmierung, Verifikation, dann vielleicht eine Intervention und dann vor allem ein Lessons Learned im Blick – das können wir alles umsetzen. Das ist auch nicht zwingend ein Superproblem, denn der Witz an der Sache ist ja, wir sagen zum Beispiel beim Drogenhandel nicht: Oh nein, wir können nicht alle harten Rauschgifte in Deutschland komplett außenvor halten, na dann fangen wir besser gar nichts mehr an, weil wir es ja nicht schaffen. Natürlich haben wir trotzdem Leute, die gegen Drogenhandel vorgehen und entsprechende Möglichkeiten kriegen. Und nein, die sind nicht immer eine „Silver Bullet“, wir kriegen keine 100 Prozent Sicherheit. Aber bei der Detektion und bei der Meldung haben wir Optionen. Wir können die Meldungen natürlich auch so aufbereiten, dass sie maschinenlesbar sind, als Datenbank. Das European Repository of Cyber Incidents macht eine freiwillige Datenbank, in der man für sich selbst ein Lagebild extrahieren kann oder die Daten extrahiert und ins eigene Lagebild, also ins eigene Risikomanagement integriert und fragt, was es denn da gibt auf dem Markt, was so bekannt geworden ist. Für die Kommunen gibt es von Jens Lange die Webseite. Es gibt so viele freiwillige Möglichkeiten, die können wir alle nutzen, anstatt zu sagen: Na ja, dann machen wir halt nichts bei den Drohnen und hoffen irgendwie, dass der Kelch an uns vorbeigeht. Es gibt noch ganz, ganz viele Steigerungen von schmutzigen Drohnen, von Kamikaze Drohnen, von Bestückung mit entsprechend explosivem Material, sogar mit Zeitverzögerung, damit, wenn sie unkontrolliert abstürzt, sie dann auch wirklich ins Terminal hineinkracht oder in Flüssiggas-Terminals oder wo auch immer. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank für die Beantwortung. Wir sind damit am Ende der zweiten Fraktionsrunde und haben es 15.29 Uhr. Wir schaffen noch eine weitere. Ich schaue zu den Fraktionen: Die Unionsfraktion nickt, die AfD-Fraktion auch. Dann steigen wir in eine weitere Fraktionsrunde ein. Ich darf auch hier für die Unionsfraktion Herrn Schmidt das Wort geben.

Abg. **Sebastian Schmidt** (CDU/CSU): Herr Vorsitzender, meine Damen und Herren. Eine Frage an Herrn Böswetter zu den Transparenzpflichten von KRITIS-Unternehmen. Sie hatten das in Ihrem Eingangsstatement schon erwähnt und deshalb noch einmal die Frage dazu: Welche Risiken ergeben sich aus den aktuellen Transparenzpflichten oder der Verfügbarkeit von sicherheitsrelevanten Informationen über Online-Ressourcen, über den Schutz und die Resilienz kritischer Infrastrukturen?

SV **Mathias Böswetter** (BDEW): Vielen Dank für diese Frage. Für uns ein ganz wichtiger Punkt, um die Resilienz in den kritischen Infrastrukturen auch nachhaltig zu steigern. Es gibt eine Reihe von Themen, die einerseits mit gesetzlichen Transparenzpflichten zusammenhängen, wo die Betreiber kritischer Infrastrukturen aufgrund von Themen etwa aus Raumordnungs- oder Planfeststellungsverfahren, Umweltverträglichkeitsprüfungen, Öffentlichkeitsbeteiligungen, aber auch Anforderungen an Transparenzpflichten aus der EU, sowie eben auch Ausschreibungs- und Vergabeverfahren relativ kritische Informationen teilen müssen. Das reicht von Geodaten über Leistungsdaten bis hin aber eben auch zu Unternehmensdaten, die dann eher aus dem Cyber- und

Informationsraum ein wichtiger Vektor sind. Hier muss man wirklich schauen, wie man vor dem Hintergrund der aktuellen sicherheits-politischen Lage diese Transparenzpflichten auch bewertet und überlegen, wie man hier auf der einen Seite das durchaus noch berechtigte Interesse einer Transparenz abwägt gegen den Schaden, den man damit anrichten kann. Ein gutes Beispiel ist das Thema Drohnen. Wir haben es jetzt auch häufiger in der Ukraine gesehen. Viele der Drohnen, die dort zum Einsatz kommen, sind vorprogrammiert. Vieles, was genutzt wird, sind eben auch Daten, die öffentlich zugänglich sind. Wir dürfen hier auch in Zukunft möglichen Bedrohungen durch Sabotage-Drohnen nicht vorbauen, indem wir hier die Daten öffentlich verfügbar machen.

Vielleicht auch noch einmal ein anderer Punkt: Wir haben eine Reihe von Beteiligungen der Verbände und der Branchen im Rahmen von Konsultationen gehabt, wo eben auch sicherheitsrelevante Informationen abgefragt wurden oder Bestandteil waren. Auch hier muss man in Zukunft schauen, wie man Beteiligungen, Verbändebeteiligungen und auch Ausschreibungen eben nur dem kritisch betroffenen Kern zugänglich macht. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Böswetter. Wir fahren fort mit der AfD-Fraktion. Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank, Herr Vorsitzender. Ich habe eine Frage an zwei Sachverständige, zum einen Herr Averhoff und Herr Stuffrein: Unsere Kommunen sind an ihren Belastungsgrenzen angekommen. Wir wissen, dass ein Großteil unserer Kommunen mittlerweile nicht mehr weiß, wie sie nächstes Jahr einen Haushalt aufstellen sollen. Sicherheit ist nicht unbedingt billig. Aus dem Grund meine Frage: Wie hoch schätzen Sie den tatsächlichen wirtschaftlichen Erfüllungsaufwand für die Implementierung dieses Gesetzes für die Kommunen ein? Insbesondere unter der Maßgabe, wie wir mit der jetzigen Gesetzeslage aufgestellt sind und wo wir noch hinwollen, wenn wir das Ganze dann noch ausweiten. Haben Sie da einen Blick? Vielleicht können Sie uns da erleuchten. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Eine Frage an die beiden Vertreter der Kommunalen Spitzenverbände. Zunächst Herr Averhoff.

SV **Alexander Averhoff** (DStGB): Vielen Dank für die Frage. Ich hatte es schon ausgeführt, dass die kommunale Finanzsituation sehr schlecht ist. Das Rekordminus, das wir bisher hatten, war 1992, da waren es 8,6 Milliarden Euro. Und in diesem Jahr haben wir ungefähr 30 Milliarden Euro – einfach, um das einmal ins Größenverhältnis zu setzen. Deswegen war auch mein Plädoyer dafür, diese zusätzlichen Belastungen zum jetzigen Zeitpunkt zumindest nicht für kleinere Betreiber vorzusehen. Eine Schätzung kann ich nicht abgeben. Da kann ich nichts Seriöses sagen. Aber der Entwurf adressiert bereits zusätzliche Aufwendungen in den kommunalen Haushalten, das erkennt er ja bereits an. Und deswegen muss das in irgendeiner Form auch im Haushalt, vielleicht auch im Bundeshaushalt, Berücksichtigung finden, um die kommunalen Haus-halte an der Stelle zu entlasten. Aber eine Quantifizierung der Mehraufwendungen hat der Gesetzgeber schon nicht drin – und können wir auch nicht machen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Stuffrein.

SV **Christian Stuffrein** (DLT): Danke. Eine Schätzung können wir auch nicht vornehmen. Letztlich hängt das auch von der noch ausstehenden Rechtsverordnung ab, welche Erfüllungsaufwände dann auch die kommunale Ebene treffen werden. Letztlich muss man sich die Abwägungsfrage stellen, was uns die Sicherheit in der gesamtstaatlichen Verwaltung wert ist. Im Bereich der NIS-2-Umsetzung hat man gesagt, gut, die Kommunen lassen wir unter den Tisch fallen. Da waren die Gespräche auch im IT-Planungsrat recht schnell vorbei, als das Wort Konnexität gefallen ist. Aus diesem Kreis müssen wir aber endlich ausbrechen, damit wir gemeinsam mit Bund, Ländern und Kommunen hier einen Weg finden, wie wir auf der Ebene vorankommen, um diesen Teufelskreis an einem gewissen Punkt durchbrechen zu können. So kommen wir nicht weiter und erzeugen eher Stillstand statt Fortschritt und das tut dem Land an der Stelle auf jeden Fall nicht gut. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Stuffrein. Für die SPD-Fraktion, Frau Nasr.

Abg. **Rasha Nasr** (SPD): Vielen Dank, Herr Vorsitzender. Wir hätten noch eine Frage, die wir gern Frau Borcherding und Herrn Prof. Dr. Kipker stellen würden: Es geht immer wieder um einheitliche Begriffsdefinitionen, Beschreibungen, Begriffs-

bestimmungen, die kritisiert werden. Herr Prof. Kipker, Sie hatten es zum Schluss noch einmal angebracht. Könnten Sie da bitte noch etwas konkreter werden, also welche Definitionen und Begriffsbestimmungen aus dem Gesetzentwurf betrifft es konkret? Das könnte uns wahrscheinlich sehr gut helfen, wenn wir jetzt weiterverhandeln. Danke schön.

SVe **Sylvia Borcherding** (50Hertz): Ich glaube, im Grundsatz ist klar, dass einheitliche Begriffe dabei helfen, möglichst wenig Reibungsverluste bei der Implementierung der Gesetzgebung zu haben. Wenn wir anfangen, darüber zu diskutieren, ob wir alle dasselbe verstehen oder Menschen sich hinter irgendwelchen Definitionen oder Begriffsbestimmungen verstecken, dann verlieren wir einfach Zeit und vielleicht auch an der ein- oder anderen Stelle die Lust. Ich mache ein Beispiel: Die Begrifflichkeit „kritische Infrastruktur“ versus „kritische Anlage“ – das wäre so ein Aspekt, wo wir glauben, dass man in eine einheitliche Begrifflichkeit einsteigen müsste. Da gibt es noch viele andere, die ich jetzt im Detail gar nicht spezifizieren will, aber im Grundsatz: Einheitliche Sprache wird sehr helfen, Reibungsverluste zu vermeiden!

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Vielen Dank für die Frage, das ist eine sehr gute Frage. Ich hatte das in meiner Stellungnahme an verschiedenen Stellen angegeben. Einerseits diese Frage nach der Definition von „kritischer Anlage“, da würde ich absolut zustimmen. Wir haben an verschiedenen Stellen auch noch keinen Gleichlauf zwischen den zwei Richtlinien der Umsetzung von CER. Das Besondere hatte ich mit dem Thema der Einrichtung der Bundesverwaltung aufgegriffen, weil wir da natürlich eine sehr kurz gewählte Definition im § 2 Nr. 10 haben und lediglich ein ganz kleiner Ausschnitt der tatsächlichen Bundesverwaltung erfasst wird. Wir haben eben auch schon mehrfach über die Relevanz der Verwaltung gesprochen für die Versorgung der Bevölkerung und der nachgelagerten Infrastrukturen. Das Problem ist, außerhalb dieser engen Definition bleiben sämtliche nachgeordneten Behörden weitestgehend außen vor. Man kann natürlich jetzt darüber diskutieren, was jetzt Bundesverwaltung, was nicht Bundesverwaltung ist. Aber gemeinhin kann man schon sagen, dass Bundesverwaltung letztendlich alle Behörden und Einrichtungen des Bundes sind, die mit dem Vollzug von Bundesaufgaben betraut sind. Da sind wir in einem Bereich, der weit über diesen Vorschlag im § 2 Nr. 10 hinausgeht. Und es werden eben die nachgelagerten, einem Ressort nachgeordneten Behörden ausgeblendet, das haben wir zurzeit definitiv so. Bundesober- und Bundesmittelbehörden – da hat Herr Atug eben auch noch einmal explizit darauf Bezug genommen –, aber wir haben auch die mittelbare Bundesverwaltung, die überhaupt nicht berücksichtigt wird, also bundesunmittelbare Körperschaften, Anstalten, Stiftungen des öffentlichen Rechts; und da werden ja gerade auch in vielen Fällen versorgungsrelevante kritische Dienstleistungen erbracht oder zentrale Unterstützungsfunktion für die Funktionsfähigkeit des Bundes wahrgenommen. Da würde ich mir einfach wünschen, dass man zumindest in diesem Bereich, wenn man jetzt schon sagt, wir können nicht eine komplette europarechtsgleiche Definition verwenden, zumindest nachzieht und diese erheblichen Vollzugsdefizite dann auch beseitigt. Danke.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Dr. von Notz, bitte.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Noch eine Frage an Herrn Kipker, ganz nah dran an dem, was Sie eben ausgeführt haben. Sie kritisieren ja auch den Regelschwellenwert des § 5. Und vielleicht können Sie noch einmal darlegen, inwiefern das problematisch ist, gerade mit Blick auf die Herleitung und die Einheitlichkeit mit den Vorgaben aus NIS-2.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Herr Kipker.

SV **Prof. Dr. Dennis-Kenji Kipker** (Universität Bremen): Also, da würde ich mich auch im Wesentlichen dem anschließen, was meine Vorredner gesagt haben. Danke für die Frage. Dieser Schwellenwert von 500 000 zu versorgenden Einwohnern, der ist einfach historisch aus dem ersten IT-Sicherheitsgesetz übernommen. Damals gab es die sogenannten BSI-Sektor-Studien. Das wurde aber nie wirklich empirisch auf eine bestimmte Art und Weise gegengeprüft und bildet meiner Meinung nach mittlerweile, wo wir immer stärker von vernetzter Infrastruktur sprechen, die Realität nicht ab. Das betrifft unter anderem wieder den anlagenbezogenen Begriff, worüber wir eben schon gesprochen haben,

weil Kaskadeneffekte im Bereich der kritischen Infrastruktur nicht berücksichtigt werden. Das ist aber etwas, was wir in unserer Forschung einfach stärker aufnehmen werden. Und wir haben teilweise auch durch diese Bezugnahme auf diesen abstrakten Schwellenwert das Risiko einer strukturellen Untererfassung. Das heißt, in Flächenländern können zum Beispiel mehrere Anlagen unterhalb des Schwellenwerts liegen, deren kombinierter Ausfall dann aber sehr gravierende Folgen hätte.

Wir haben aber nicht nur mit dem Schwellenwert an sich Probleme, sondern auch bei den Ausnahmeregelungen. Darauf bin ich auch in meiner Stellungnahme eingegangen. Beispielsweise, wir haben hier Einzelfallfeststellungen des BMI, die können zwar ganz interessant sein, aber am Ende haben wir einen sehr weitreichenden Ermessensspielraum, wo man sagen kann, das ist eben eine kritische Infrastruktur im Sinne des KRITIS-Dachgesetzes oder nicht, ohne dass das wirklich nachvollziehbar wäre. Und wir haben auch eine unzureichende Transparenz bei diesen ganzen ergänzenden Kriterien, wo wir über wissenschaftliche Evidenz sprechen. Wenn man in den § 5 Absatz 2 beispielsweise hineinschaut, da heißt es: „… Dauer und Ausmaß, mögliche Auswirkungen, Marktanteil des Betreibers…“. Das ist an der Stelle weitestgehend unpräzise. Und wenn wir eben sagen wollen, wir wollen den Betreiberinnen oder Betreibern auch hinreichende Rechtssicherheit an die Hand geben, ohne dass sie umfassende Prüfaufwände etc. hatten, dann müssen wir diese Leitlinien einfach viel näher konkretisieren, ansonsten haben wir am Ende vielleicht sogar noch, wenn man das in die Praxis umsetzt, eine sehr heterogene Behördenumsetzungspraxis. Und das schadet am Ende natürlich einem einheitlichen KRITIS-Niveau in Deutschland. Danke.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Aber das BMI scheint an diese Zahl zu glauben. Vielleicht kann man das ja einmal aus der Anhörung mitnehmen.

Amt. Vors. **Josef Oster** (CDU/CSU): Wir hören uns alle gegenseitig zu und jeder nimmt das mit, was er hier für relevant hält. Vielen Dank. Es bleibt die Fraktion Die Linke. Herr Köstering, haben Sie noch eine Frage?

Abg. **Jan Köstering** (Die Linke): Herr Vorsitzender, vielen Dank. Noch zum Abschluss eine Frage an Herrn Atug. Sowohl in Ihrer Stellungnahme als auch in der des Bundesrates wird moniert, dass einzelne Sektoren in der Liste der kritischen Einrichtungen nicht aufgezählt sind, obwohl sie durch-aus für die Aufrechterhaltung von Staat und Gesellschaft relevant, also kritisch, sind. Welche Sektoren sind da aus Ihrer Sicht unterschätzt?

Amt. Vors. **Josef Oster** (CDU/CSU): Herr Atug.

SV **Manuel Atug** (AG KRITIS): Ja, wir haben mindestens natürlich den Sektor Staat und Verwaltung, der erheblich defizitär ist. Dann haben wir noch Medien und Kultur, die sind ja auch jeweils Bundesländereinigungsthema – auch da haben wir bei NIS-2 schon irgendwie jahrelang erfolglos diskutiert und gesagt, naja, man könnte ja eine einheitliche Bundesländermusterverordnung machen, wo man Staat und Verwaltung, Medien und Kultur auf der Länderebene regelt, alle einigen sich auf ein Verfahren, eine Vorgabe, dann gibt es keine Differenzen und jeder muss an dasselbe ran. Auch da hat jedes Bundesland gesagt: Naja, das machen wir dann irgendwie anders. Und wenn man in den Einzelgesprächen war, wurde gesagt: Hat denn schon ein anderes Bundesland irgendwie sowas oder so? Nicht? Also ja, dann ist gut, dann machen wir auch nichts. Also insofern wartet man da auch irgendwie auf die Erlösung oder aufs Geld, denn ohne Geld wird da nichts umgesetzt. Dann hat das BBK selbst schon seit vielen, vielen Jahren, lange bevor KRITIS überhaupt definiert wurde, schon eine KRITIS-Begrifflichkeit und benennt da eben auch ganz klar Großforschungseinrichtungen und den Sektor Chemie als wesentliche kritische Infrastruktur, die dann auch Störfälle erheblichen Ausmaßes erbringen, Massenanfall von Verletzten verursachen kann etc. Auch diese zwei Sektoren haben wir immer wieder angesprochen und gesagt, ob man das vielleicht in der BSI-KRITIS-Verordnung für die Cybersicherheit adressieren möchte. Im KRITIS-Dachgesetz sind ja erhebliche Mängel an den Definitionen und auch diese beiden finden sich dann natürlich ganz klar wieder. Insofern sind auch das große Mängel, die fehlen. Man könnte natürlich auch überlegen, ob man ein Parlament oder einen Bundestag mit dazu packt, wäre nebenbei auch wegzucybern oder kann sich nicht vor Sturzregen oder sonstigen Vorfällen schützen. Auch da kann man darüber nachdenken, wie handlungsfähig wir eigentlich sind, wenn das nicht mehr funktioniert. Wenn man das im Gedankengang verwirklicht, dann weiß man auch, warum diese Dinge vielleicht

doch kritisch für ein funktionales Versorgungsgeschehen einer Demokratie sind.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, meine Damen, meine Herren. Für eine vollwertige Fragerunde reicht die Zeit nicht. Gibt es noch eine Frage, die zwingend noch gestellt werden sollte? Das sehe ich nicht. Dann sind wir mit dieser Anhörung heute am Ende. Ich darf mich nochmals sehr herzlich bei unseren Sachverständigen bedanken für Ihre Bereitschaft, dem Deutschen Bundestag mit Ihrer Expertise zur Verfügung zu stehen. Mir ist es immer wichtig, mich dafür zu bedanken, weil ich weiß, dass der Deutsche Bundestag, was jetzt eine Aufwandsentscheidung anbetrifft, recht knauserig mit seinen Sachverständigen umgeht. Dafür macht man das also nicht, Sie machen das aus Überzeugung. Deshalb ist es mir besonders wichtig, Ihnen allen dafür herzlich zu danken. Ich glaube, es ist deutlich geworden, dass das Thema drängt, dass es eigentlich jeden Tag bedeutender wird. Das nehmen wir als Parlamentarier natürlich mit. Die Sitzung ist geschlossen. Ich wünsche Ihnen allen einen schönen Abend und eine gute Woche.

Schluss der Sitzung: 15.45 Uhr

Josef Oster, MdB
Amtierender Vorsitzender