Verband kommunaler Unternehmen e.V.
Invalidenstraße 91
10115 Berlin

www.vku.de

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Berlin, 14. Februar 2023

Stellungnahme zum Eckpunktepapier KRITIS-Dachgesetz

Transparenz-Register-ID des BDEW: 20457441380-38
Transparenz-Register-ID des VKU: 1420587986-32

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten über 1.900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 90 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Der Verband kommunaler Unternehmen e. V. (VKU) vertritt über 1.500 Stadtwerke und kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit rund 283.000 Beschäftigten wurden 2019 Umsatzerlöse von 123 Milliarden Euro erwirtschaftet und mehr als 13 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 62 Prozent, Gas 67 Prozent, Trinkwasser 91 Prozent, Wärme 79 Prozent, Abwasser 45 Prozent. Sie entsorgen jeden Tag 31.500 Tonnen Abfall und tragen durch getrennte Sammlung entscheidend dazu bei, dass Deutschland mit 67 Prozent die höchste Recyclingquote in der Europäischen Union hat. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau: 203 Unternehmen investieren pro Jahr über 700 Millionen Euro. Beim Breitbandausbau setzen 92 Prozent der Unternehmen auf Glasfaser bis mindestens ins Gebäude. Wir halten Deutschland am Laufen – klimaneutral, leistungsstark, lebenswert. Unser Beitrag für heute und morgen: #Daseinsvorsorge. Unsere Positionen: 2030plus.vku.de.

Einleitung

Der BDEW und der VKU begrüßen grundsätzlich die Impulse des Eckpunktepapiers zum KRITIS-Dachgesetz für den physischen Schutz Kritischer Infrastrukturen. Auch wir sehen im Vergleich zur Cybersichersicherheitsregulierung in vielen Sektoren erheblichen Nachholbedarf beim physischen Schutz Kritischer Infrastrukturen. Vor dem Hintergrund des russischen Angriffskriegs haben die Sabotageakte auf die Nord Stream-Pipelines oder auf die Lichtwellenleiterkabel der Deutschen Bahn gezeigt, wie verletzlich Kritische Infrastrukturen gegenwärtig gegenüber physischen Angriffen sind.

Das zukünftige KRITIS-Dachgesetz soll als Umsetzung der CER-Richtlinie dabei aber nicht nur den physischen Schutz Kritischer Infrastrukturen regeln, sondern im Zusammenhang mit dem Fünf-Punkte-Plan der Europäischen Kommission[1] auch einer neuen Bedrohungsintensität begegnen, die sich aus einem hochprofessionellen Täterprofil und der Bedrohung von zivilen Infrastrukturen durch hybride Bedrohungen ergibt. Hybride Bedrohungen sind verschiedene Formen illegitimer Einflussnahme auf Staaten und Gesellschaften durch fremde Staaten. Physische Bedrohungen und Cyberbedrohungen sind zunächst den sogenannten hybriden Bedrohungen zuzuordnen, wenn sie direkt oder indirekt durch fremde Staaten gesteuert werden. Physische Bedrohungen und Cyberbedrohungen sind darüber hinaus den sogenannten hybriden Bedrohungen zuzuordnen, wenn diese in Intensität und Qualität die völkerrechtliche Definition von kriegerischen Handlungen unterlaufen, dabei aber in der Summe erheblichen politischen, gesellschaftlichen oder wirtschaftlichen Schaden erzeugen können.[2] Um die Wirkung zu maximieren und gleichzeitig das Risiko zu minimieren, den Schwellenwert von kriegerischen Handlungen zu überschreiten, werden dabei bei hybriden Bedrohungen verschiedene Bedrohungsräume verschaltet und miteinander verschnitten (etwa Cyberraum, physischer Raum oder Informationsraum).

Vor diesem Hintergrund bedarf es auch eines konvergenten und ganzheitlichen Ansatzes für das Meldewesen, die Lagebeurteilung und die Mitigation, der alle für den sicheren Betrieb von Kritischen Infrastrukturen einschlägigen Bedrohungsräumen umfassend berücksichtigt. Insbesondere im Zusammenhang mit der Beurteilung der Systemsicherheit müssen die zuständigen Behörden auch die komplexen sowie reziproken cyber-physischen Wechselwirkungen bei Netz- und Erzeugungsinfrastruktur beurteilen können.

[1] Kommission ruft Mitgliedstaaten zu besserem Schutz kritischer Infrastrukturen auf (europa.eu)

[2] Vgl. Kilcullen, David. (2019). The Evolution of Unconventional Warfare. Scandinavian Journal of Military Studies. 2. 61-71. 10.31374/sjms.35.

Position von BDEW und VKU im Überblick

Um diesen Ansprüchen gerecht werden zu können, hat ein zukünftiges KRITIS-Dachgesetz aus unserer Sicht folgende Anforderungen zu erfüllen:

1. Die Harmonisierung der Regulierung zur Cybersicherheit und des physischen Schutzes sowie die Identifizierung geeigneter branchenspezifischen Anforderungen an die physische Sicherheit sind entscheidend für die effektive Umsetzbarkeit durch die KRITIS Betreiber. Die Identifizierung geeigneter Schutzmaßnahmen kann nur in Zusammenarbeit mit den Betreibern bzw. Betreiberverbänden erfolgen.
2. Verhältnismäßige Transparenz- und Auskunftspflichten für Betreiber Kritischer Infrastrukturen und Schutzdieser Informationen auf der behördlichen Seite.
3. Es ist eine Konkretisierung notwendig, was unter den kritischen Komponenten, die keine IT-Komponenten im Sinne des BSIG sind, zu verstehen ist. Die zukünftige Regulierung zu den kritischen Komponenten darf deren Beschaffung nicht über Gebühr erschweren.
4. Es müssen geeignete Behördenzuständigkeiten geschaffen und die behördenübergreifende Zusammenarbeit gesichert werden. Das BBK muss entsprechend finanziell und personell ausgestattet werden, um seiner neuen Zuständigkeit auch gerecht werden zu können.
5. Das Melde- und Nachweiswesen muss vereinheitlicht bzw. in bestehende Prozesse integriert werden. Die Betreiber Kritischer Infrastrukturen müssen insbesondere Sicherheitsvorfälle zentral an nur eine Stelle melden können und nur so kann beim Staat ein einheitliches und ganzheitliches Lagebild entstehen. Ein Vorfall, eine Meldung!
6. Die einheitliche Umsetzung der zukünftigen Regelungen zum physischen Schutz Kritischer Infrastrukturen auf Bundes-, Landes- und Kreisebene muss sichergestellt werden.
7. Die Abwehr staatlicher Akteure oder terroristischer Vereinigungen kann durch die Betreiber Kritischer Infrastrukturen nicht umgesetzt werden und stößt auch im Sinne geeigneter Abwehr- bzw. Abschreckungsmechanismen an bestehende rechtliche Grenzen. Hier hat der Staat eine besondere Verantwortung zur Unterstützung der Betreiber.

Ausführliche Stellungnahme von BDEW und VKU

1. Harmonisierung von Cybersicherheitsregulierung und Regulierung des physischen Schutzes für die effektive Umsetzbarkeit

Das zukünftige KRITIS-Dachgesetz soll nach den Eckpunkten die Vorgaben der CER-Richtlinie umsetzen und hat damit den physischen Schutz Kritischer Infrastrukturen zum Gegenstand. Eine Harmonisierung mit der Umsetzung der NIS 2.0-Richtlinie, dem Cyber Resilience Act oder spezialrechtlichen Regelungen (z.B. Network Code on Cybersecurity, IT-Sicherheitskataloge gemäß § 11 Absatz 1a und § 11 Absatz 1b EnWG oder Kritische Komponenten nach §11 Abs.1g EnWG) ist entscheidend für eine effektive und wirtschaftliche Umsetzbarkeit.

Es muss dabei unbedingt vermieden werden, dass die Anforderungen an Betreiber Kritischer Infrastrukturen und die Compliance-Nachweise nicht oder nur ungenügend mit den bestehenden Vorgaben aus der bestehenden Cybersicherheitsregulierung harmonisiert werden (etwa durch unterschiedliche Zertifizierungszyklen). Dadurch würden nicht nur zusätzliche, sondern auch ganz neuartige Anforderungen auf die Betreiber Kritischer Infrastrukturen zukommen, die etwa vor dem Hintergrund begrenzter Ressourcen (u.a. personell aufgrund von Fachkräftemangel, oder auch von begrenzten wirtschaftlichen Spielräumen) bei ungenügender Harmonisierung kaum erfüllt werden können. Darüber hinaus muss darauf geachtet werden, dass bereits bestehende Detail-Reglungen nicht erneut, ggf. sogar widersprechend geregelt werden (Vermeidung von Mehrfachregulierung). Deshalb ist es unabdingbar, früh genug, umfassend und unverzichtbar Betreiber und Bertreiberverbände in die Ausgestaltung der Anforderungen im KRITIS-Dachgesetz mit einzubeziehen. Dabei müssen die bisherigen und in den Verbänden vorliegenden Erfahrungen aus vorherigen Regulierungs- und Gesetzgebungsverfahren (z.B. Smart Meter Gateway, Systeme zur Angriffserkennung) berücksichtigt werden. Neue Anforderungen müssen die Möglichkeit bieten, in bestehende Managementsysteme (z.B. gemäß IT-Sicherheitskataloge, ISO/IEC 27001 oder Branchenstandards) integriert zu werden. Nur hierdurch kann eine verhältnismäßige Regulierung sichergestellt werden. Abschließend ist zu bemerken, dass sowohl das Datenschutzrecht als auch die betriebliche Mitbestimmung die erforderlichen Maßnahmen zum Schutz der Kritischer Infrastrukturen erschweren können. So kann beispielsweise die Video- oder Zutrittsüberwachung von Grundstücken mit dem Datenschutz der Arbeitnehmer kollidieren. Auch die betriebliche Mitbestimmung kann bestimmte Maßnahmen zum Schutz der kritischen Infrastrukturen schwierig durchsetzbar machen. Entscheidend ist, dass durch das KRITIS-Dachgesetz keine Pflichten aufgestellt werden, die mit diesen Regelungen kollidieren.

2. Zusammenspiel von Risikobewertung, Resilienzplänen, Schutzstandards und spezifischen Regelungen

KRITIS-Betreiber müssen ihre spezifischen Schutzmaßnahmen an den im Rahmen eines betrieblichen Risikomanagements durchzuführenden Risikobewertungen und an den zu definierenden europaweit einheitlichen Mindestvorgaben (verpflichtende Schutzstandards) ausrichten. Die spezifischen Schutzmaßnahmen sollen dabei geeignet und angemessen sein. Darüber hinaus wird die Erstellung von Resilienzplänen für die stetige Erhöhung der Resilienz gefordert. Offen bleibt jedoch, wer für die Erstellung dieser Resilienzplänen verantwortlich ist und wie das Zusammenspiel dieser Resilienzpläne, der aus den Risikobewertungen resultierenden Risikobehandlungspläne, dem stetig anzupassenden verpflichtenden europaweiten Schutzstandard und den zutreffenden weitergehenden sektorspezifischen Regelungen aussehen kann. Um den Betreibern der kritischen Infrastrukturen die anvisierte Orientierung und Handlungssicherheit zu geben, muss dieser Prozess detaillierter ausformuliert werden. Gegenwärtig fehlt in diesem Zusammenhang auch ein integrierter Ansatz, der Sicherheit ganzheitlich denkt und in die Umsetzung bringt (integriertes Sicherheitsmanagementsystem). Der Entwurf leistet vielmehr einem „Silodenken“ Vorschub, der in Deutschland bestehenden Trennung von physischen und digitalen Risiken und entsprechenden

Schutzmaßnahmen. Ein zukünftiges KRITIS-Dachgesetz muss die Themenbereiche einer ganzheitlichen Sicherheit einrahmen, um eine umfassende, abgestimmte Regelungslage zu schaffen und damit eine effiziente Umsetzung bei den KRITIS-Betreibern zu ermöglichen. Sofern ein Unternehmen ein integriertes Sicherheitsmanagementsystem für alle Sicherheitsthemen betreibt (z.B. basierend auf gesetzlichen IT-Sicherheitskatalogen, der ISO/IEC 27001 oder Branchenstandards), ist die wechselseitige Anerkennung eines diesbezüglichen einzelnen Nachweises (z.B. Zertifikats) bei den unterschiedlichen Aufsichtsbehörden (im Energiesektor z.B.: BBK, BSI, BNetzA) zu ermöglichen, damit Mehrfachzertifizierungen für die KRITIS-Betreiber ausgeschlossen werden.

3. Verhältnismäßige Transparenz- und Auskunftspflichten

Wie die oben genannten Sabotageakte gezeigt haben, stellt die Bereitstellung von sensiblen Daten, die Aufschluss über Sicherheitsmaßnahmen und kritische Prozesse Kritischer Infrastrukturen geben, ein erhebliches und essenzielles Risiko für den zuverlässigen und sicheren Betrieb Kritischer Infrastrukturen dar.

Gegenwärtig unterliegen Betreiber Kritischer Infrastrukturen einer Vielzahl von Informationsfreiheits- und Transparenzgesetzen sowohl auf Ebene des Bundes als auch auf Ebene der Länder (auf Bundesebene z.B. das IFG, das GeoZG und das UIG). Darüber hinaus bestehen aber auch speziellere Normen, die eine Datenherausgabe anordnen. Beispielsweise ist hier § 79 Abs. 2 S. 1 TKG zu nennen. Danach verlangt die zentrale Informationsstelle des Bundes von Eigentümern oder Betreibern öffentlicher Versorgungsnetze, die über Einrichtungen verfügen, die zu Telekommunikationszwecken genutzt werden können, diejenigen Informationen, die über Art, gegenwärtige Nutzung sowie tatsächliche Verfügbarkeit und geografische Lage des Standortes und der Leitungswege dieser Einrichtungen erforderlich sind. Zwar wird hiervon nach § 79 Abs. 3 Nr. 3 TKG eine Ausnahme für Kritische Infrastrukturen angeordnet. Allerdings müssen gleichwohl diese Informationen zunächst an die zentrale Informationsstelle gesendet werden und sodann ein Ausnahmeantrag gestellt werden damit diese Informationen nicht veröffentlicht werden.

Insgesamt sollte sichergestellt werden, dass Informationen über die Kritischen Infrastrukturen nicht zu einfach über die Informationsfreiheits- und Transparenzgesetze zugänglich sind. Im Rahmen des KRITIS-Dachgesetzes sollten KRITIS-Betreiber von den vielen und weitreichenden gesetzlichen Transparenzpflichten ohne Stellung eines Antrags ausgenommen werden. Zudem sollte – wie im Fall des § 79 Abs. 3 Nr. 3 TKG – die Information über Kritische Infrastrukturen nicht an einem zentralen Punkt gesammelt und gespeichert werden, bevor über ihre Veröffentlichung konkret entschieden wird. So würden an einem einzigen Punkt sensible Informationen zusammenlaufen und ein „Single Point of Failure“ entstehen. Wird diese zentrale Informationsstelle kompromittiert, besteht Zugriff auf eine Vielzahl von Informationen über Kritische Infrastrukturen von einer Vielzahl von Betreibern.

Zusätzlich sind Auskunftspflichten und die Bereitstellungen von Dokumenten und Listen insbesondere im Rahmen von Zertifizierungsverfahren im Rahmen des KRITIS-Dachgesetzes kritisch zu hinterfragen. Bspw. wird zunehmend bei Zertifizierungsverfahren gemäß IT-Sicherheitskatalog die Herausgabe von vollständigen Listen der kritischen Informationswerte (Hardwarelisten) und Listen

nicht dauerhaft besetzter Standorte durch die Zertifizierer gefordert. Dies steht im Konflikt zum Schutz vertraulicher und sensibler Daten, da an zentralen Stellen sensible Daten mehrere Betreiber gesammelt werden und damit das Risiko einer unbeabsichtigten Veröffentlichung erhöht wird.

4. Beschaffungsvorbehalte bei kritischen Komponenten, die keine IT-Komponenten im Sinne des BSIG sind, dürfen Beschaffungsprozesse nicht unverhältnismäßig erschweren

Die zukünftige Regulierung zur Beschaffung von kritischen Komponenten analog zum IT-Sicherheitsgesetz würde auch hier von der Einholung möglicher Garantieerklärung für kritische Komponenten, über deren Administration und den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes, zu Lasten der Betreiber gehen. Es besteht die Gefahr, dass das Vorhaben durch etwaige Zwangsvorgaben in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen eingreift und könnte ggf. zu Marktverzerrungen wegen Ungleichbehandlung führen. Die Kriterien zur Auswahl von einsetzbaren kritischen Komponenten müssen zwingend mit den Betreibern bzw. Betreiberverbänden festgelegt und kommuniziert werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Sicherheit auch im Gefahrenfall zu ermöglichen. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss verhältnismäßig und unter Wahrung einer ausreichenden Übergangsfrist erfolgen (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr, die Sicherheit in Kritischen Infrastrukturen zu schwächen. Die Beschaffbarkeit kritischer Komponenten ist essenziell für die Versorgungssicherheit. Bei vorliegenden Versorgungsengpässen für kritische Komponenten sollte eine Güterabwägung zwischen Konformität der Vorgaben für kritische Komponenten und der Versorgungssicherheit im Sinne der Beschaffung erfolgen.

Darüber hinaus sollte im zukünftigen KRITIS-Dachgesetz konkretisiert werden, was unter den kritischen Komponenten, die keine IT-Komponenten im Sinne des BSIG sind, zu verstehen ist. Mit der im Eckpunktepapier gegebenen Definition, könnten auch Baumaterialien und Rohstoffe unter eine Bestimmung kritischer Komponenten im Sinne des zukünftigen KRITIS-Dachgesetz fallen. Eine Definition sollte bei der Bestimmung der Kritikalität nur auf die Erbringung der kritischen Dienstleistung durch die betrachtete Komponente abstellen.

5. Geeignete Behördenzuständigkeit und behördenübergreifende Zusammenarbeit

Die Bundeszuständigkeit im zukünftigen KRITIS-Dachgesetz soll laut den Eckpunktepapier beim BBK liegen, das als übergeordnete KRITIS-Behörde im Sinne des zukünftigen Dachgesetzes erst noch aufgestellt werden muss. Dazu müssten die Befugnisse des BBK deutlich erweitert werden und zusätzliche finanzielle und personelle Mittel bereitgestellt werden. Da das KRITIS-Dachgesetz gegenwärtig noch unter dem Finanzierungsvorbehalt steht, besteht das Risiko, dass das BBK seiner neuen Aufgabe nicht gerecht werden kann. Daneben gibt es weitere Zuständigkeiten, die sich aus den spezialrechtlichen Regelungen etwa des Energiewirtschaftsgesetzes ergeben und die mit

eigenen Anforderungen an die technische Gestaltung von Kritischer Infrastruktur einhergehen bzw. einhergehen werden. Branchenspezifische Schutzmaßnahmen sind sinnvoll, es muss jedoch sichergestellt werden, dass keine widersprüchlichen Anforderungen gestellt werden und konkurrierende Zuständigkeiten sowie Interessen der Behörden entstehen, die in der Praxis zu nicht auflösbaren bzw. nur mit unverhältnismäßigem Aufwand auflösbaren Problemen führen.

6. Meldewesen von herausragender Bedeutung

Insbesondere vor dem Hintergrund der steigenden Bedeutung hybrider Bedrohungen, in denen Informationsraum, Cyberraum und physischer Raum orchestriert „verschnitten“ werden und dabei gerade keiner dieser Bedrohungsräume aus Angreifersicht einen wesentlichen Vorrang hat, muss ein KRITIS-Dachgesetz die Zuständigkeiten für alle möglichen Bedrohungsräume auch unter einer Behörde oder einer effektiven behördenübergreifenden Zusammenarbeit bündeln können. Dies gilt insbesondere für das zukünftige Meldewesen.

Das IT-Sicherheitsgesetz sieht z.B. vor, dass für die Meldung von IT-Sicherheitsvorfällen mit dem BSI eine zentrale Meldestelle besteht, die diese dann unter der Berücksichtigung sektorspezifischer Merkmale von Vorfällen an die zuständigen Fachbehörden auf Bundes- oder Landesebene weiterleitet. Dieses Vorgehen hat sich bisher bewährt und muss in ähnlicher Weise in einem Ansatz fortgeschrieben werden, in dem physischer Schutz und Cyberschutz in einem ganzheitlichen Melde- und Lagebildwesen zusammengeführt werden. In diesem Zusammenhang ist auch die Einrichtung eines behördenübergreifenden nationalen Sicherheitslagezentrums in Erwägung zu ziehen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z.B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte.

7. Einheitliche Umsetzung der Regelungen auf Bundes-, Landes- und Kreisebene

Die Erfahrung aus der Corona-Pandemie hat gezeigt, dass die Abstimmung zwischen Bund, Ländern, Landkreisen sowie Kommunen oftmals von großen Reibungsverlusten, unterschiedlichen Auslegungen und der Umsetzungen der Vorschriften gekennzeichnet war. Ein konkretes Beispiel hierfür war die unterschiedliche Ausstellungspraxis von KRITIS-Bescheinigungen durch die Landkreisämter bzw. Ministerien. In vielen Fällen war auch unklar, wer diese KRITIS-Bescheinigungen ausstellt. Ein zukünftiges KRITIS-Dachgesetz sollte aus dieser Erfahrung Lehren ziehen, um klare und einheitliche Regelungen, Zuständigkeiten sowie Umsetzungen zu schaffen.

8. Staat in der Pflicht bei der Abwehr von hochprofessionellen Tätern und hybriden Bedrohungen

Das Eckpunktepapier betont die besondere Verantwortung des Staates. Dieser Verantwortung soll der Staat durch das Angebot von Analysen, Leitfäden, Beratung, Übungen und Schulungen für die Betreiber Kritischer Infrastrukturen nachkommen.

Darüber hinaus sollte die besondere staatliche Verantwortung aber auch in der Abwehr von staatlich organisierten bzw. hybriden Anschlägen- oder Sabotageakten liegen. Die im Eckpunktepapier erwähnte und im Verantwortungsbereich der KRITIS-Sektoren liegende Umsetzung geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen sowie von Sicherheitsmaßnahmen für die jeweilige privatwirtschaftliche Einrichtung sollte sich damit nicht auf die Abwehr staatlich organisierter bzw. hybrider Bedrohungen beziehen. Die Abwehr staatlicher Akteure kann durch die KRITIS-Sektoren erstens nicht verhältnismäßig umgesetzt werden und stößt zweitens auch im Sinne geeigneter Abwehr- bzw. Abschreckungsmechanismen an bestehende rechtliche Grenzen (z.B. Drohnenabwehr oder der Einsatz militärischer Abwehrsysteme).

Ferner müssen die Voraussetzungen geschaffen werden, damit die im Eckpunktepapier erwähnten Maßnahmen auch umgesetzt werden können. Dies betrifft insbesondere den für den Cyberschutz und physischen Schutz gleichermaßen wichtigen Aspekt der Sicherheitsüberprüfungen. Hier liegt es an den zuständigen Bundesbehörden, endlich die notwendigen Ressourcen bereitzustellen.

9. Neuregelung der Gefahrenabwehr erforderlich

Obwohl das Eckpunktepapier betont, dass das Gesamtsystem beim physischen Schutz Kritischer Infrastrukturen im Vordergrund stehen muss, erwähnt das Papier leider nicht die aus Sicht eines Bundesgesetzes wesentliche Herausforderung, dass die Gefahrenabwehr im Sinne dieser Gesamtsystemperspektive und der neuen Bedrohungsintensität nicht mehr durch die alleinige Zuständigkeit der Länder erfolgen kann, sondern in Zukunft unter Beteiligung von Bundesbehörden und vor dem Hintergrund des Fünf-Punkte-Plans der Europäischen Kommission sogar durch europäische oder militärische Organisationen wie der NATO erfolgen muss.

Außerhalb von NIS 2.0- und CER-Richtlinie muss der zukünftige Schutz Kritischer Infrastrukturen auch die sicherheitspolitischen Risiken von strategischen Partnerschaften und gesellschaftsrechtlichen Übernahmen Kritischer Infrastrukturen durch Drittstaaten angemessen berücksichtigen.