Autorinnenpapier von

Dr. Irene Mihalic, MdB
Erste Parlamentarische Geschäftsführerin
Fraktion Bündnis 90/Die Grünen im
Deutschen Bundestag

Dr. Julia Höller, MdL
Stellvertretende Fraktionsvorsitzende
Sprecherin für Innenpolitik
Fraktion Bündnis 90/Die Grünen im Landtag NRW

Schutz Kritischer Infrastrukturen: Sieben Punkte für ein KRITIS-Dachgesetz

Kritische Infrastrukturen (KRITIS) sind die Grundpfeiler und Lebensadern unserer Gesellschaft, indem sie die Versorgung mit lebensnotwendigen Gütern und Dienstleistungen gewährleisten. Wenn Kritische Infrastrukturen ausfallen oder nur begrenzt funktionsfähig sind, führt dies innerhalb von wenigen Tagen zu erheblichen Versorgungsengpässen und zu Einschränkungen im öffentlichen Leben und bei den Bürgerinnen und Bürgern.

Wir Grüne fordern daher schon seit vielen Jahren, den Schutz Kritischer Infrastrukturen ernst zu nehmen und in der sicherheitspolitischen Agenda mit höchster Priorität auf die Tagesordnung zu setzen. Zentrale Risiken wurden viel zu lange sträflich vernachlässigt. Rechtliche Rahmenbedingungen müssen nun endlich geschaffen und notwendige Investitionen dringend getätigt werden. Und dabei gilt: Sicherheit gibt es auch bei KRITIS nicht zum Nulltarif. Bund und Länder müssen im Rahmen ihrer Zuständigkeiten Basis-Investitionen tätigen und sich auch danach an entsprechender Förderung der Wirtschaft, insbesondere mittelständischer Betriebe beteiligen.

Der völkerrechtswidrige Angriffskrieg des Putin-Regimes gegen die Ukraine, die dadurch ausgelösten sicherheitspolitischen Herausforderungen wie drohende Energieengpässe, die Sorge vor großflächigen, langanhaltenden Stromausfällen (Blackouts), sowie die Sprengung der Gas-Pipelines Nord Stream 1 und 2 in der Ostsee und die Sabotage an Kabeln bei der Deutschen Bahn, zeigen die unbedingte Notwendigkeit den physischen Schutz von KRITIS zu verstärken. Darüber hinaus stehen Kritische Infrastrukturen vor der immensen Herausforderung Personalengpässe durch die Corona Pandemie zu bewältigen. Zudem ist die Bedrohungslage von Cyberangriffen weiterhin sehr hoch.

Der Schutz Kritischer Infrastrukturen liegt in der gemeinsamen Verantwortung des Staates – also des Bundes und der Ländern – und der KRITIS-Betreiber. Der Bund ist gefordert, mit einem KRITIS-Dachgesetz einen rechtlichen Rahmen vorzugeben, der die regulative Basis für den physischen Schutz Kritischer Infrastrukturen definiert. Obwohl es für den Schutz Kritischer Infrastrukturen mit Bezug zur Informationssicherheit bereits eine komplexe Regulatorik gibt, fehlt diese für den physischen Schutz Kritischer Infrastrukturen komplett. Einzelne rechtliche Fragestellungen sind bisher in Fachgesetzen, Normungen und Standards geregelt, die aber nicht aufeinander abgestimmt sind. Ein verbindlicher normativer sektoren-

und branchenübergreifender Ansatz zum physischen Schutz von Kritischen Infrastrukturen fehlt bisher.

Ein KRITIS-Dachgesetz ist daher unbedingt notwendig, um Rechtssicherheit für die handelnden Akteure zu schaffen, Prävention verbindlich zu machen und Schadenslagen effektiver managen zu können. Angesichts der sich zuspitzenden Lage drängt die Zeit.

Bundesinnenministerin Nancy Faeser hat bereits im Sommer dieses Jahres angekündigt Eckpunkte für ein KRITIS-Dachgesetz vorzulegen, so wie es im Koalitionsvertrag der Ampel vereinbart wurde. Für die Formulierung eines solchen Gesetzes sind die folgenden Punkte unverzichtbar.

Sieben Punkte, die in einem KRITIS-Dachgesetz geregelt werden müssen

1. Legaldefinition für Kritische Infrastrukturen festlegen

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) reguliert KRITIS-Sektoren und legt Kritische Infrastrukturen im Sinne dieses Gesetzes in der BSI-Kritisverordnung fest. Die dort definierten kritischen Dienstleistungen und Schwellenwerte beziehen sich jedoch ausschließlich auf den Bereich der Informationssicherheit. Unter anderem der Sabotageakt auf das Funknetz der Deutschen Bahn hat gezeigt, dass die aktuellen Gesetze für den physischen Schutz kritischer Infrastrukturen noch nicht ausreichen. Insbesondere braucht es eine Legaldefinition von Kritischen Infrastrukturen, die jenseits einer zwar allgemein anerkannten, aber unverbindlichen Definition des Bundesinnenministeriums (BMI)[1] endlich Rechtssicherheit schafft. Ein KRITIS-Dachgesetz muss diese Leerstelle schnell und Sektor für Sektor ausfüllen und Handlungs- und Definitionssicherheit schaffen.

2. Verantwortungen und Zuständigkeiten verbindlich regeln

Der Schutz KRITIS ist in Deutschland gemeinsame Aufgabe von Staat (Bund und Länder) und Wirtschaft. Dieser „kooperative Ansatz“ hat in den letzten 15 Jahren einen wesentlichen Beitrag zur Versorgungssicherheit mit kritischen Gütern und Dienstleistungen in Deutschland geleistet und muss nun weiterentwickelt werden, gerade den physischen Schutz Kritischer Infrastrukturen betreffend. Es gilt, die gemeinsame Verantwortung, die Rechte und Pflichten der staatlichen Akteure verbindlich zu regeln, um Handlungssicherheit zu schaffen.

Dabei muss auch die Zusammenarbeit auf europäischer Ebene mit in den Blick genommen und geregelt werden. Denn auch die EU-Kommission hat unlängst eine Empfehlung an den EU-Rat zur Resilienz Kritischer Infrastrukturen ausgesprochen. Die Empfehlung sieht eine stärkere Unterstützungs- und Koordinierungsfunktion der Kommission vor sowie eine verstärkte Zusammenarbeit zwischen den Mitgliedsstaaten (und deren Nachbarländern) in den Schlüsselbereichen Energie, digitale Infrastruktur, Verkehr und Raumfahrt. Die Empfehlung sieht u.a. die Durchführung von Stresstests auf Basis gemeinsamer Grundsätze,

[1] https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html#:~:text=Kritische%20Infrastrukturen%20sind%20Einrichtungen%2C%20Anlagen,f%C3%BCr%20die%20%C3%B6ffentliche%20Sicherheit%20eintreten.

die Ausarbeitung eines Konzeptpapiers zu Sicherheitsvorfällen und Krisen bei Kritischer Infrastruktur, sowie die Einrichtung einer EU-NATO Taskforce zu Kritischer Infrastruktur im strukturierten Dialog der Institutionen vor. Zudem setzt sich die EU-Kommission dafür ein, dass die Mitgliedsstaaten die kürzlich beschlossene Richtlinie zum Schutz Kritischer Infrastruktur (CER-RL) und die Cybersicherheits-RL (NIS 2-RL) beschleunigt umsetzen.

3. Vorsorge und Prävention sektorübergreifend bundesweit regeln

Ob ein Stromausfall für den direkten Ausfall der Kritischen Infrastruktur sorgt, ist heute abhängig von dem persönlichen Interesse und Investitionswillen des Betreibers. Ob Redundanzen, also Rückfallebenen geschaffen, Notstromaggregate angeschafft werden oder besonders sensible Bereiche besser geschützt werden – all das liegt im Ermessen der Unternehmen. Die enormen Interdependenzen – also Abhängigkeiten – zwischen den Infrastrukturen machen ein einheitliches Präventionsniveau notwendig, damit Störungen im Kleinen nicht zum Systemausfall im Großen führen.

4. Standards für das Risiko- und Krisenmanagement und verbindliche Definition von Schutzzielen festlegen

Welche KRITIS wie lange mit Treibstoff für den Dieselgenerator versorgt ist, ob überhaupt eine Notstromversorgung vorhanden ist und wie lange die Versorgung mit kritischen Dienstleistungen aufrechterhalten werden kann, all das ist weder branchenspezifisch einheitlich geregelt noch gibt es für staatliche Hilfeleistungssysteme wie Feuerwehren, Rettungsdienste oder Hilfsorganisationen Einblicke und Übersichten in die Durchhaltefähigkeit der Kritischen Infrastrukturen.

Im KRITIS-Dachgesetz müssen Standards zum Risiko- und Krisenmanagement festgelegt werden, die sektoren- und branchenübergreifend gültig sind. Dies betrifft administrative Strukturen, aber auch Vorhaltezeiten und Schutzziele. Die Frage „wie gut wollen wir uns schützen?“ ist nicht einfach zu beantworten, muss aber politisch und akteursübergreifend ausgehandelt werden.

Professionelles Krisenmanagement folgt einheitlichen Regeln. Diese müssen gelernt und umgesetzt werden. Dafür braucht es verbindliche Regelungen. Bisher gibt es jenseits der BSI-Kritisverordnung keine definierten Schutzziele oder Schutzstandards. Dementsprechend sind die KRITIS-Betreiber sehr heterogen aufgestellt und die Frage „wie gut sind wir geschützt?“ ist aktuell nicht belastbar zu beantworten. Damit staatliche Maßnahmen diesen Schutz wirkungsvoll ergänzen können, müssen einheitliche Schutzstandards etabliert werden.

5. Finanzierung von Schutzmaßnahmen neu aufstellen

In das KRITIS-Dachgesetz müssen kluge Förder- und Finanzierungsmöglichkeiten aufgenommen werden. Beispiel für erfolgreiche Förderstrukturen sind die Förderungen des Bundes im Rahmen der Wassersicherstellung zur Erhöhung der Versorgungssicherheit. Auch Fördermaßnahmen zur Beschaffung von z.B. Notstromaggregaten oder sonstige physischen Schutzmaßnahmen (z.B. Einbruchssichere Türen, verstärkte Panzerung oder

Absicherung von wichtigen Räumen oder Kabeln und Leitungssträngen) sollten jenseits des Wassersicherstellungsgesetzes durch den Bund möglich sein. Dafür braucht es eine angepasste Rechtslage.

6. Gesamtlagebild ermöglichen

Wie in vielen Bereichen der Sicherheitspolitik verfügen wir auch mit Blick auf Kritische Infrastrukturen nur über lückenhafte Kenntnisse zu den Auswirkungen verschiedener plausibler Szenarien. Bisher gibt es keine Möglichkeit für ein übergeordnetes staatliches Krisenmanagement, bei dem auf verlässliche Daten über die Versorgungssituation mit kritischen Gütern und Dienstleistungen in der Krise zugegriffen werden kann. Die Informationslage ist sehr uneinheitlich. Es müssen daher mit Bezug auf die Versorgungssicherheit Meldepflichten für Unternehmen oder staatlichen Gebietskörperschaften festgelegt werden, um in einer Krisenlage schnell handeln zu können.

7. Hybride Gefährdungen ernst nehmen – physischen Schutz und Informationssicherheit zusammen denken!

Wenn wir von kritischen Infrastrukturen sprechen, meinen wir sowohl sichtbare Komponenten, wie Kraftwerke, Krankenhäuser, Kläranlagen, Umspannwerke, Netzknoten, Rechenzentren oder Wasserleitungen als auch unsichtbare Komponenten mit Blick auf den „Cyberraum“. Angriffe erfolgen auf sichtbare und unsichtbare Bestandteile der KRITIS, oft auch auf Beides. Das KRITIS-Dachgesetz muss daher dringend auch hybride Gefahren berücksichtigen. Es ist zu überlegen, inwiefern physische Gefahren, also der konkrete, sichtbare Angriff auf Kritische Infrastrukturen und Gefahren die Informationssicherheit betreffend, zum Beispiel das Abschöpfen von Informationen aus Datensystemen oder deren Manipulation, gemeinsam gesetzlich geregelt werden können. Sofern dies nicht möglich ist, muss dafür gesorgt werden, dass die gesetzlichen Regelungen bestmöglich aufeinander abgestimmt sind.

Berlin/Düsseldorf, den 25. Oktober 2022