126. FDP-Landesparteitag, 21. November 2026

Antragsteller:
Hendrik Korb, Sami Musa

Drs.: ___/___

Ja
Nein
Enthaltungen

Angenommen
Ja
Nein
Überwiesen

Kritische Infrastruktur besser gegen Sabotage, Spionage und Drohnen schützen, Rechtssicherheit für Betreiber schaffen

Der Landesparteitag möge beschließen:

Die FDP Hamburg fordert einen besseren Schutz von für das Funktionieren des Gemeinwesens essentiellen Einrichtungen. Dazu gehören insbesondere Anlagen der Energie-, Wasser- und Lebensmittelversorgung, IT und Telekommunikation, des Gesundheits-, Finanz-, Transport- und Verkehrswesens sowie der Abfallentsorgung. Sie werden als Kritische Infrastrukturen, kurz KRITIS, bezeichnet. Ihr Schutz vor Sabotage, Spionage, Drohnenangriffen und anderen gezielten Störungen muss im Alltag funktionieren. Dafür sollen das KRITIS-Dachgesetz (KRITISDachG) und die für die Drohnenabwehr nötigen Vorschriften gezielt verbessert werden.

Für die Abwehr von Gefahren bleibt der Staat verantwortlich. Betreiber müssen bspw. verdächtige Drohnen jedoch erkennen und melden können. Betreiber besonders gefährdeter Anlagen brauchen außerdem eine eng begrenzte Möglichkeit, bei unmittelbarer Gefahr selbst einzugreifen, wenn staatliche Hilfe nicht rechtzeitig kommt. Neue Behörden, zusätzliche Verzeichnisse und doppelte Meldungen lehnen wir ab.

Schützen, was für die Versorgung wichtig ist

Ob eine Anlage besonderen Schutz braucht, muss von den Folgen ihres Ausfalls abhängen. Ihre Größe oder die Zahl der versorgten Menschen allein reichen als Maßstab nicht aus. Der Wert von 500.000 versorgten Einwohnern soll eine Anlage gemäß KRITISDachG automatisch als erheblich schutzbedürftig einstufen. Anlagen unterhalb dieses Wertes dürfen aber nicht ausgeschlossen werden. Auch sie müssen verbindlich eingestuft werden können, wenn ihr Ausfall schwere Folgen hätte.

Dabei muss berücksichtigt werden, ob ein Ausfall weitere Ausfälle in der Region auslösen würde, ob Krankenhäuser oder Pflegeeinrichtungen von der Anlage abhängen und ob kurzfristig Ersatz verfügbar ist. Auch Anlagen, die wichtige Produkte für Sicherheit und Verteidigung liefern, müssen berücksichtigt werden. Erfasst werden soll jeweils die wichtige Anlage, nicht pauschal das gesamte Unternehmen.

Länder und Betreiber sollen die Einstufung in einem einfachen Verfahren überprüfen lassen können. Die zuständige Behörde muss innerhalb einer kurzen, festgelegten Frist entscheiden. Dafür sind bestehende Behörden und das vorhandene Verzeichnis für Kritische Infrastrukturen zu nutzen.

Verdächtige Drohnen erkennen und melden

Betreiber brauchen klare Rahmenvorgaben, damit sie verdächtige Drohnen frühzeitig erkennen und melden können. Es muss eindeutig sein, welche Informationen sie dafür erfassen, auswerten, speichern und an Behörden weitergeben dürfen.

Betreiber der erfassten Anlagen sollen in einem klar abgegrenzten Bereich Geräte zur Drohnenerkennung einsetzen dürfen. Technische Informationen und Bilder, die zur Einschätzung eines Vorfalls nötig sind, müssen sie verarbeiten und sofort an die zuständigen Behörden weitergeben können.

Diese Informationen dürfen nur dem Schutz der Anlage, der Alarmierung und der Sicherung von Beweisen dienen. Nicht benötigte Daten sind zeitnah zu löschen. Eine allgemeine Überwachung öffentlicher Straßen und Plätze ist damit ebenso wenig erlaubt wie ein Eingriff in erlaubte Drohnenflüge oder -fahrten.

Bei unmittelbarer Gefahr handeln können

Drohnen abzuwehren bleibt grundsätzlich Aufgabe des Staates. Die Verantwortung dafür darf nicht auf private Betreiber übertragen werden.

Für vorher festgelegte, besonders gefährdete Anlagen soll es jedoch eine gesetzliche Ausnahme für den Notfall geben. Sie darf nur greifen, wenn Menschen, die Versorgung oder der Betrieb der Anlage unmittelbar gefährdet sind und die Polizei oder andere zuständige staatliche Kräfte erkennbar nicht rechtzeitig eingreifen können.

Erlaubt sein dürfen nur vorher genehmigte technische Maßnahmen, die auf einen engen Bereich begrenzt sind. Wenn dies technisch sicher möglich ist, kann beispielsweise eine Drohne kontrolliert übernommen und (an)gelandet oder mit einem Fangsystem aufgehalten werden. Schusswaffen, Sprengmittel, großflächige Störsender und selbstständig handelnde Waffensysteme bleiben ausgeschlossen.

Nur geschultes und zugelassenes Personal darf eingreifen. Jeder Einsatz muss automatisch aufgezeichnet und sofort gemeldet werden. Vorab muss klar geregelt sein, wer für Schäden haftet, welche Versicherung nötig ist und wo die Grenzen des Eingreifens liegen.

Einmal melden und schnell Hilfe bekommen

Bei akuter Gefahr zählt jede Minute. Eine Meldung innerhalb von 24 Stunden ersetzt deshalb keinen Notruf. Jedes Bundesland soll eine bestehende, rund um die Uhr erreichbare Leitstelle als zentrale Anlaufstelle für akute Vorfälle benennen. Betreiber melden den Vorfall einmal. Die Leitstelle gibt die Informationen automatisch an die zuständige Polizeidienststelle und weitere erforderliche Stellen weiter. Den Einsatz leitet weiterhin die gesetzlich zuständige Behörde.

Bei Drohnenvorfällen soll auch das Gemeinsame Drohnenabwehrzentrum die nötigen Informationen erhalten. Es soll Informationen aus den Ländern zusammenführen, Zusammenhänge erkennen und die Zusammenarbeit der Behörden unterstützen. Der Einsatz vor Ort darf dadurch nicht verzögert werden.

Die zuständige Stelle der Bundeswehr im jeweiligen Bundesland soll einbezogen werden, wenn ein Vorfall die Verteidigung Deutschlands oder seiner Bündnispartner, militärische Transporte oder eine mögliche Unterstützung hierbei durch zivile Behörden und Unternehmen betrifft. Sie erhält die nötigen Informationen; die Zuständigkeit der zivilen Behörden bleibt bestehen.

Warnungen und Meldungen müssen auch dann ankommen, wenn Mobilfunk oder Internet ausfallen. Vorrangig soll dafür das besonders ausfallsichere Funknetz für Kritische Infrastrukturen genutzt werden, das sogenannte 450-Megahertz-Funknetz. Berechtigte Betreiber müssen darüber wichtige Warnungen und Meldungen mit Vorrang senden können. Wo ein Zugang technisch nicht möglich ist, muss ein vergleichbarer, unabhängiger Ersatzweg bereitstehen.

Die gemeinsame Meldemöglichkeit der Bundesämter für Bevölkerungsschutz und für IT-Sicherheit soll nach dem Grundsatz „einmal melden, mehrfach nutzen“ ausgebaut werden. Bereits übermittelte Daten, bestehende Prüfungen und anerkannte Nachweise dürfen nicht erneut verlangt werden.

Begründung

Für die Menschen zählt, ob Strom, Wasser und andere wichtige Leistungen verfügbar bleiben. Auch eine kleinere kritische Anlage kann für einen ganzen Stadtteil, Bezirk oder eine Region entscheidend sein. Fällt etwa ein Umspannwerk aus, können hiervon Krankenhäuser, Pflegeeinrichtungen und viele Betriebe betroffen sein. Ein Ausfall bspw. von Teilen des Hamburger Hafens hätte teils verheerende Folgen für viele Menschen und Unternehmen überall in Deutschland und anderswo in Europa. Auch deshalb fordert der Zentralverband deutscher Seehafenbetriebe (ZDS) einen klaren Rechtsrahmen für die Drohnenabwehr zu Wasser, zu Lande und in der Luft.

Ebenso wichtig können zudem spezialisierte Anlagen sein, deren Produkte u.a. für Sicherheit und Verteidigung kurzfristig nicht ersetzt werden können. Deshalb darf besonderer Schutz nicht allein von einer Einwohnerzahl abhängen, sondern bedarf weiterer Kriterien.

Gemeinsame Regeln für den Schutz wichtiger Anlagen sind daher sinnvoll. KRITIS-Anlagen-Betreiber müssen Risiken prüfen und sich auf Ausfälle vorbereiten. Dazu brauchen sie aber auch klare Befugnisse. Gerade bei verdächtigen Drohnen muss für Betreiber vorab feststehen, welche Informationen sie nutzen dürfen und was sie bei einer unmittelbaren Gefahr tun können.

Bei einem Drohnenangriff kann die Zeit bis zum Eintreffen staatlicher Hilfe zu lang sein. Besonders gefährdete Anlagen brauchen deshalb klare Regeln für den Notfall. Verantwortung und Grenzen müssen feststehen, bevor etwas passiert.

Die eng begrenzte Ausnahme gibt ausgewählten Betreibern eine letzte Handlungsmöglichkeit, wenn eine Gefahr unmittelbar bevorsteht. Sie gilt nur, wenn staatliche Hilfe nicht rechtzeitig eingreifen kann. Genehmigte Maßnahmen und zugelassenes Personal stellen sicher, dass die Verantwortung des Staates gewahrt bleibt.

Ebenso wichtig ist ein schneller und zuverlässiger Meldeweg. Ein Formular mit einer Frist von 24 Stunden sorgt noch nicht dafür, dass Hilfe in den nächsten Minuten eintrifft. Auch bei einem Ausfall von Mobilfunk oder Internet müssen Betreiber die zuständigen Stellen erreichen können. Dafür sollen das besonders ausfallsichere Funknetz und unabhängige Ersatzwege genutzt werden.

Der Vorschlag nutzt vorhandene Leitstellen, Meldesysteme, Behörden und Kommunikationsnetze. Die Informationen gelangen zu den Stellen, die sie benötigen. So lässt sich schneller reagieren, ohne neue Behörden oder doppelte Arbeit zu schaffen.

Wer Betreibern Verantwortung auferlegt, muss ihnen klare und angemessene Handlungsmöglichkeiten geben. Zugleich muss staatliche Hilfe schnell erreichbar sein. So schützen wir die Versorgung der Menschen wirksam und ohne unnötige Bürokratie.