10.08.2026

Positionspapier des ZDS

Deutschland besser vor Drohnen schützen:

Ein 10-Punkte-Plan des ZDS für den Schutz kritischer Infrastrukturen in Luft und Wasser

Der Drohnenvorfall am Flughafen Leipzig ist ein Warnschuss. Er zeigt: Deutschland hat beim Schutz kritischer Infrastrukturen wichtige rechtliche und politische Schritte auf den Weg gebracht. Die KRITIS-Gesetzgebung, erweiterte Befugnisse der Sicherheitsbehörden und höhere Anforderungen an Betreiber gehen in die richtige Richtung. Doch der Praxistest offenbart weiterhin eine entscheidende Lücke: Zwischen der **Erkennung einer Bedrohung und ihrer wirksamen Abwehr** liegen zu viele ungeklärte Zuständigkeiten, technische Brüche und operative Defizite.

Diese Lücke muss geschlossen werden. Dabei darf die Debatte nicht auf Flughäfen und den Luftraum beschränkt bleiben. Deutschland muss Drohnenabwehr umfassender denken. Neben unbemannten Fluggeräten gewinnen auch **unbemannte Systeme auf und unter Wasser** an Bedeutung. Gerade für Seehäfen, maritime Verkehrswege, Energieanlagen, Pipelines, Kabel, Kaianlagen und militärisch relevante Infrastruktur entsteht damit ein zusätzliches Gefährdungspotenzial.

Deutschland braucht deshalb ein integriertes Schutzkonzept gegen unbemannte Systeme **in der Luft, auf dem Wasser und unter Wasser**. Die deutschen Seehäfen sollten dafür zu einem Praxistest werden. Denn kaum irgendwo zeigt sich die Herausforderung deutlicher.

Seehäfen sind kritische Infrastruktur von nationaler und europäischer Bedeutung. Sie sichern Warenströme, Energieversorgung, industrielle Produktion und Außenhandel. Zugleich wächst ihre Bedeutung für die militärische Mobilität Deutschlands und seiner NATO-Partner. LNG-Terminals, Energieanlagen, Containerterminals, Bahn- und Straßenverbindungen, Kommunikationsinfrastruktur und militärisch nutzbare Umschlagflächen liegen teilweise auf engem Raum nebeneinander.

Gleichzeitig treffen in den Häfen besonders viele Zuständigkeiten aufeinander: Bund, Länder und Kommunen, Polizei- und Sicherheitsbehörden, Bundeswehr, Hafenbehörden und private Betreiber.

Genau deshalb sind die Seehäfen ein **Lackmustest für die Handlungsfähigkeit des Staates beim Schutz kritischer Infrastruktur**.

Der ZDS schlägt deshalb einen **10-Punkte-Plan für eine neue Architektur der Drohnenabwehr** vor:

1. Drohnenabwehr als gesamtstaatliche Aufgabe organisieren:

Der Schutz kritischer Infrastruktur darf nicht an föderalen oder institutionellen Zuständigkeitsgrenzen scheitern. Deutschland braucht ein verbindliches Gesamtkonzept, das festlegt, **wer erkennt, wer bewertet, wer entscheidet und wer abwehrt**. Für kritische Infrastrukturen müssen Bund und Länder gemeinsame Einsatz- und Reaktionsketten definieren. Für jeden relevanten Standort muss bereits vor einem Zwischenfall eindeutig feststehen, welche Behörde wann die Verantwortung übernimmt. Gerade die Seehäfen eignen sich aufgrund ihrer komplexen Zuständigkeitsstruktur als Modellregionen für solche Strukturen.

2. Ein flächendeckendes Lagebild schaffen:

Wirksame Abwehr beginnt mit zuverlässiger Detektion. Deutschland braucht deshalb ein möglichst lückenloses Lagebild über verdächtige unbemannte Systeme im Umfeld kritischer Infrastruktur.

Dafür müssen geeignete Sensoren unterschiedlicher Technologien miteinander vernetzt werden. Betreiber kritischer Infrastrukturen können und sollen hierzu einen Beitrag leisten. Es ist grundsätzlich zumutbar, dass KRITIS-Betreiber definierte Detektions- und Sensortechnik installieren und betreiben, vorausgesetzt, sie erhalten dafür den erforderlichen rechtlichen, technologischen und finanziellen Rahmen. Entscheidend ist jedoch: **Der Staat muss Standards definieren und die Vernetzung sicherstellen.** Es darf kein Flickenteppich inkompatibler Einzellösungen entstehen. Sensoren an Häfen, Flughäfen, Energieanlagen und anderen kritischen Standorten müssen technisch so ausgelegt sein, dass relevante Informationen in ein übergeordnetes Lagebild einfließen können.

3. Regionale staatliche Leitstellen aufbauen:

Detektionsdaten allein schaffen noch keine Sicherheit. Sie müssen zusammengeführt, ausgewertet und mit anderen Lageinformationen verknüpft werden. Deutschland sollte deshalb regionale, staatlich geführte Leitstellen für die Abwehr unbemannter Systeme schaffen oder bestehende Strukturen entsprechend ertüchtigen. Dort müssen Informationen aus KRITIS-Sensorik, Polizei, Bundeswehr und bestehender Luftraumüberwachung zusammenlaufen. Für den maritimen Bereich müssen zusätzlich Daten über Bewegungen auf und unter Wasser integriert werden. Das Ziel ist ein **gemeinsames Echtzeit-Lagebild statt vieler isolierter Einzelbilder**.

4. KI für Erkennung, Bewertung und Reaktion nutzen:

Bei modernen Drohnensystemen können zwischen Detektion und notwendiger Reaktion nur Sekunden oder wenige Minuten liegen. Eine rein manuelle Verarbeitung der Informationen stößt dabei schnell an Grenzen. Deutschland braucht deshalb leistungsfähige, KI-gestützte Systeme, die Detektionsdaten automatisiert zusammenführen, Flug- oder Bewegungsbahnen prognostizieren und Objekte kategorisieren können.

Ein solches System sollte unter anderem beurteilen können:

- Um welchen Typ unbemannten Systems handelt es sich?
- Wie verhält es sich und welches Ziel könnte es ansteuern?
- Welche technische Ausstattung ist erkennbar oder wahrscheinlich?
- Welche Abwehrmöglichkeiten stehen zur Verfügung?
- Wo könnte eine Abwehr mit möglichst geringem Risiko für Dritte erfolgen?

Die Entscheidung über besonders eingriffsintensive Maßnahmen muss dabei in einer klar definierten staatlichen Verantwortung verbleiben. **Automatisierung muss staatliche Handlungsfähigkeit erhöhen, nicht staatliche Verantwortung ersetzen.**

5. Detektion und Abwehr endlich zusammenbringen:

Die größte Schwäche des heutigen Systems liegt zwischen Erkennen und Handeln. Es reicht nicht, wenn ein Hafenbetreiber eine Drohne erkennt, dokumentiert und anschließend lediglich die zuständige Behörde verständigen kann, während wertvolle Zeit verstreicht. Für KRITIS-Standorte müssen deshalb verbindliche Reaktionsketten mit definierten Reaktionszeiten geschaffen werden. Dazu gehören Übungen, gemeinsame Lagebilder und bereits im Vorfeld festgelegte Verantwortlichkeiten. **Eine Drohne zu erkennen, ohne sie im Ernstfall rechtzeitig abwehren zu können, schafft noch keine Sicherheit.**

6. Staatliches Gewaltmonopol erhalten. Betreiber zugleich zur Abwehr befähigen:

Das staatliche Gewaltmonopol muss auch bei der Drohnenabwehr grundsätzlich erhalten bleiben. Insbesondere Maßnahmen, die erhebliche Gefahren für unbeteiligte Dritte mit sich bringen können, müssen staatlichen Stellen vorbehalten sein. Der Staat trägt die Verantwortung dafür, dass solche Eingriffe geeignet, erforderlich und verhältnismäßig sind.

Zur Realität gehört jedoch auch: **Der Staat wird auf absehbare Zeit nicht in der Lage sein, sämtliche kritischen Infrastrukturen in Deutschland jederzeit und vollumfänglich gegen Drohnen zu schützen.** Gerade weitläufige und komplexe Infrastrukturen wie Seehäfen machen deutlich, dass eine ausschließlich staatliche Abwehr in der Praxis an personelle, technische und operative Grenzen stößt. Deshalb muss neben der staatlichen Abwehr eine klar geregelte **Eigenbefähigung der Betreiber kritischer Infrastrukturen** treten. Betreiber sollten unter definierten Voraussetzungen in die Lage versetzt werden, bestimmte niedrigschwellige und risikoarme Maßnahmen zur Abwehr von Drohnen eigenständig einzusetzen. Wo die Gefährdung von Menschen oder erhebliche Kollateralschäden nicht ausgeschlossen werden können, muss die Entscheidungshoheit dagegen beim Staat verbleiben.

Dafür braucht es einen eindeutigen gesetzlichen Rahmen: Welche Maßnahmen dürfen Betreiber ergreifen? Unter welchen Voraussetzungen? Welche technischen Systeme dürfen eingesetzt werden? Wo verläuft die Grenze zwischen zulässiger privater Gefahrenabwehr und hoheitlichem Eingriff?

Zugleich müssen die Betreiber technisch und finanziell in die Lage versetzt werden, diese Aufgaben wahrzunehmen. Der Bund sollte hierfür verbindliche Standards definieren, geeignete Technologien zulassen beziehungsweise zertifizieren und für besonders sicherheitsrelevante kritische Infrastrukturen entsprechende Förderinstrumente schaffen.

Das Ziel muss eine **gestufte Sicherheitsarchitektur** sein: Betreiber erkennen Gefahren, stellen Informationen bereit und können klar definierte niedrigschwellige Abwehrmaßnahmen selbst ergreifen. Staatliche Sicherheitsbehörden übernehmen dort, wo weitergehende Eingriffe erforderlich sind. **Das staatliche Gewaltmonopol und eine stärkere Eigenbefähigung der KRITIS-Betreiber sind deshalb kein Widerspruch. Sie müssen sich ergänzen. Denn wer kritische Infrastruktur wirksam schützen will, muss auch diejenigen handlungsfähig machen, die vor Ort als Erste mit einer Bedrohung konfrontiert sind.**

7. Einen abgestuften Werkzeugkasten der Abwehr schaffen:

Nicht jede Drohne stellt dieselbe Gefahr dar. Entsprechend darf es nicht nur die Alternative zwischen Beobachten und Abschießen geben. Deutschland braucht einen abgestuften technologischen Werkzeugkasten für die Drohnenabwehr. Je nach Bedrohung, Umgebung und technischen Eigenschaften des Systems müssen unterschiedliche nicht-kinetische und – als letztes Mittel – kinetische Maßnahmen verfügbar sein. Entscheidend ist das Prinzip der **verhältnismäßigen Wirkung**: Die konkrete Gefährdung muss analysiert und dasjenige Mittel gewählt werden, das die Bedrohung zuverlässig beendet und zugleich das Risiko für Beschäftigte, Bevölkerung und Infrastruktur möglichst geringhält. Dafür müssen geeignete Effektoren an strategisch wichtigen Punkten verfügbar sein und von den zuständigen staatlichen Stellen kurzfristig eingesetzt werden können.

8. Nicht nur in die Luft schauen: maritime Drohnenabwehr aufbauen:

Die bisherige Debatte konzentriert sich zu stark auf fliegende Drohnen. Für Seehäfen greift das zu kurz. Unbemannte Systeme können sich **in der Luft, auf dem Wasser und unter Wasser** bewegen. Unterwasserdrohnen und autonome Überwassersysteme können ebenso zur Aufklärung, Sabotage oder zum Angriff auf kritische Infrastruktur eingesetzt werden. Besonders gefährdet sind Hafenbecken, Zufahrten, Schleusen, Energieanlagen, Leitungen, Kabel, Kaianlagen und militärisch relevante Infrastruktur. Dazu kommt, dass Unterwasserdrohnen auch beim Drogenschmuggel eine Rolle spielen, die bekämpft werden muss. Deutschland braucht deshalb ein **dreidimensionales Schutzkonzept für den Luftraum sowie den Oberflächen- und Unterwasserraum**. **Seehäfen sollten als Pilotstandorte genutzt** werden, um Sensorik, Lagebilder und Reaktionsketten für diese drei Dimensionen miteinander zu verbinden.

9. Seehäfen zu Modellregionen der Drohnenabwehr machen:

In den deutschen Seehäfen kommen fast alle Herausforderungen moderner KRITIS-Sicherheit zusammen: Energieversorgung, Logistik, industrielle Infrastruktur, internationale Lieferketten, zivile Schifffahrt, militärische Mobilität und komplexe föderale Zuständigkeiten. Genau deshalb sollten Bund und Länder gemeinsam mit Hafenbetreibern ausgewählte deutsche Seehäfen zu **Modellregionen für integrierte Drohnenabwehr** entwickeln.

Dort können Technologien, Datenplattformen, Zuständigkeitsmodelle und gemeinsame Einsatzkonzepte von Bund, Ländern, Bundeswehr, Landes-, Wasserschutz-, Bundespolizei, Hafenbehörden, Feuerwehr-/Rettungsdiensten und privaten Betreibern unter realen Bedingungen erprobt werden. Was unter den komplexen Bedingungen eines Seehafens funktioniert, lässt sich anschließend auch auf andere kritische Infrastrukturen übertragen.

Flankierend ist zwischen den deutschen Seehäfen, den zuständigen Sicherheitsbehörden und Organisationen ein strukturierter Informationsaustausch zu etablieren. Ziel ist die gemeinsame Bewertung neuer Bedrohungen, die Weitergabe von Erkenntnissen und die Harmonisierung von Verfahren. Dadurch ist sichergestellt, dass neue Bedrohungen, technologische Entwicklungen und gesetzliche Änderungen zeitnah berücksichtigt werden. Alle beteiligten Organisationen stellen sicher, dass ihr Personal regelmäßig fortgebildet wird. Ergänzend sind gemeinsame Übungen durchzuführen, um die Zusammenarbeit unter realistischen Bedingungen zu erproben.

10. Investitionsprogramm für KRITIS-Schutz und Drohnenabwehr auflegen:

Sicherheit gibt es nicht zum Nulltarif. Die Anforderungen an Betreiber kritischer Infrastruktur steigen erheblich. Dazu gehören Sensorik, IT-Infrastruktur, Cybersecurity, physischer Schutz und künftig zunehmend auch Systeme zur Erkennung unbemannter Flug-, Überwasser- und Unterwasserfahrzeuge. Der Staat kann verbindliche technische Mindeststandards definieren und Betreibern zumutbare Eigenleistungen auferlegen. Gleichzeitig muss er dort finanziell unterstützen, wo gesamtstaatliche Sicherheitsinteressen berührt sind oder staatliche Anforderungen erhebliche zusätzliche Investitionen auslösen. Für besonders sicherheitsrelevante Hafeninfrastruktur – insbesondere im Bereich Energieversorgung und militärischer Mobilität – braucht es deshalb ein gemeinsames Investitionsprogramm von Bund und Ländern.

Fazit:

Deutschland verfügt über einen großen Teil der Technologien, die für einen besseren Schutz kritischer Infrastruktur notwendig sind. Die entscheidende Herausforderung liegt deshalb nicht allein in technologischer Innovation.

Es geht um **Vernetzung, Geschwindigkeit, Zuständigkeit und Entscheidungsfähigkeit**.

Sensoren müssen ein gemeinsames Lagebild erzeugen. Daten müssen in Echtzeit zusammengeführt werden. KI muss dabei helfen, Bedrohungen schneller zu identifizieren und Handlungsoptionen zu bewerten. Staatliche Stellen müssen über geeignete Mittel verfügen und innerhalb klar definierter Strukturen schnell entscheiden können.

Der Vorfall von Leipzig sollte deshalb nicht als isoliertes Ereignis betrachtet werden. Er ist ein Hinweis auf eine strukturelle Verwundbarkeit. Die deutschen Seehäfen bieten die Möglichkeit, darauf eine konkrete. Antwort zu entwickeln. Sie sind aufgrund ihrer Bedeutung für Energieversorgung, Außenhandel, industrielle Wertschöpfung und militärische Mobilität einerseits besonders schutzbedürftig – und aufgrund der komplexen Zuständigkeiten andererseits ein besonders anspruchsvoller Testfall.

Wenn Deutschland die Drohnenabwehr in seinen Seehäfen organisatorisch, rechtlich und technisch zum Funktionieren bringt, schafft es damit zugleich eine Blaupause für den Schutz kritischer Infrastruktur insgesamt.

Der ZDS fordert deshalb Bund und Länder auf, gemeinsam mit der Hafenwirtschaft kurzfristig ein Pilotprogramm **„Drohnenabwehr Seehäfen“** aufzulegen. Ziel muss es sein, innerhalb eines klar definierten Zeitrahmens integrierte Detektions-, Lagebild- und Abwehrkonzepte für Bedrohungen aus der Luft sowie auf und unter Wasser praktisch zu erproben. Denn die entscheidende Frage lautet nicht mehr, ob kritische Infrastruktur durch unbemannte Systeme ausgespäht, gestört oder angegriffen werden kann.

Die entscheidende Frage ist, **ob Deutschland im Ernstfall schnell genug erkennt, entscheidet und handelt.**

Ihr Ansprechpartner beim ZDS: Florian Keisinger (+49 175 22 88 417)