

Positionspapier

Sofortpaket „Drohnenabwehr“: Maßnahmen zur kurzfristigen Verbesserung der Informationslage und des Lagebilds in der kritischen Energie- und Wasserinfrastruktur

Stand: 28.09.2026

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten mehr als 2.000 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 95 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Der BDEW ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung sowie im europäischen Transparenzregister für die Interessenvertretung gegenüber den EU-Institutionen eingetragen. Bei der Interessenvertretung legt er neben dem anerkannten Verhaltenskodex nach § 5 Absatz 3 Satz 1 LobbyRG, dem Verhaltenskodex nach dem Register der Interessenvertreter (europa.eu) auch zusätzlich die BDEW-interne Compliance Richtlinie im Sinne einer professionellen und transparenten Tätigkeit zugrunde. Registereintrag national: R000888. Registereintrag europäisch: 20457441380-38

1 Einleitung

Der Drohnen-Vorfall am Flughafen Leipzig/Halle am 4./5. August 2026 zeigt, dass sich die Gefährdungslage der kritischen Infrastrukturen durch Drohnen erhöht hat und weitere Eskalationsstufen nicht auszuschließen sind. Die kritischen Infrastrukturen der Energie- und Wasserwirtschaft sind ebenfalls seit Jahren in erheblichem Maße von Drohnenüberflügen betroffen, welche im schlimmsten Fall der Vorbereitung von Sabotage-Akten durch maliziöse Akteure dienen könnten.

In der sich verschärfenden hybriden Sicherheitslage geraten aber auch zunehmend Infrastrukturen der Energie- und Wasserwirtschaft in den Fokus von Drohnenangriffen: Ende März 2026 attackierten russische Drohnen den Interkonnektor Isaccea–Vulcănești, der die Stromsysteme von Moldau und Rumänien miteinander verbindet. In der Folge stand Moldau laut Medienberichten kurz vor einem Blackout, wenngleich dies unter höchsten Anstrengungen verhindert werden konnte. Der Vorfall in Moldau zeigt, dass lokale Störungen zu kaskadierenden und überregionalen Versorgungskrisen in Energiesystemen führen können.

Bund und Länder sollten vor diesem Hintergrund dringend einen Beitrag zur Drohnenabwehr in der kritischen Infrastruktur der Energie- und Wasserwirtschaft leisten und dabei deren besondere Voraussetzungen berücksichtigen, die gerade bei den Energienetzen durch Überregionalität und Interdependenzen bestimmt sind. Derzeit wird viel über die Zuständigkeit bei der Drohnenabwehr, insbesondere bei den in der Bundeszuständigkeit liegenden Flughäfen, diskutiert.

Dringlich ist aus Sicht der Energie- und Wasserwirtschaft jedoch insbesondere kurzfristig die vorgelagerten Ebenen der Drohnenabwehr zu adressieren. Im Rahmen des vorliegenden Positionspapiers schlagen wir daher Maßnahmen vor, die im Sinne eines Sofortpakets zeitnah zu einer Verbesserung von Informationslage und Lagebild beitragen würden. Nichtsdestotrotz gilt es auch eine baldige Klärung der Zuständigkeit der Drohnenabwehr herbeizuführen.



Übersicht: Drohnenabwehr in der kritischen Energie- und Wasserinfrastruktur

2 Sofortpaket Drohnenabwehr: Verbesserung der Informationslage und des Lagebilds

2.1 Klärung der Zuständigkeit: Bundeseinheitliche Regelung anstatt Länder-Flickenteppich

Die hybride Bedrohungslage ist ernst und umso wichtiger wird die einheitliche und verlässliche Gefahrenabwehr durch die Sicherheitsbehörden. Der BDEW möchte hiermit an die Länder appellieren: Sicherheit und Resilienz setzen klare länderübergreifende Zuständigkeiten voraus. Zur Erreichung dieses Ziels möchten wir hervorheben, dass wenngleich die allgemeine Gefahrenabwehr prinzipiell Ländersache ist, so müsste die Koordinierung und Verantwortlichkeit hinsichtlich der Drohnenabwehr zukünftig auf Bundesebene zusammengeführt werden müssen, um der Gefahrenlage effektiv begegnen zu können.

Aufgrund des bisherigen Agierens der Länder in dem Themenfeld nehmen wir wahr, dass landesgesetzliche Regelungen im Hinblick auf Drohnen keinen hinreichenden Beitrag im Krisenfall (und zu deren Prävention) leisten würden und setzen uns daher ausdrücklich für eine bundeseinheitliche Regelung der Drohnenabwehr ein. Dies sollte sowohl für die Erstellung der Lagebilder als auch für die eigentliche Abwehr gelten. Folgende Gründe sprechen aus unserer Sicht für eine Zuständigkeit auf Bundesebene:

- Viele kritische Infrastrukturen, wie z. B. Stromleitungen, haben einen überregionalen Charakter. Aufgrund von möglichen kaskadierenden Effekten kann so auch ein lokaler Vorfall zu einer überregionalen bzw. bundeslandsübergreifenden Versorgungskrise oder Störung des europäischen Verbundnetzes führen.
- Weiterhin ist im Krisenfall die Zeit der kritische Faktor: Je mehr Behörden und andere Institutionen eingebunden werden müssen, desto länger werden etwaige Entscheidungs- und Reaktionszeiten. Typischerweise bleibt zwischen Sichtung und Reaktion bzgl. Drohnen nur ein Zeitfenster von wenigen Sekunden bis Minuten.
- Ein zentraler Punkt ist aus unserer Sicht zudem die Finanzierung von Detektions- und Abwehrmaßnahmen. Würde die Drohnenabwehr auch in Zukunft primär Ländersache bleiben, dann würde hierdurch eine Finanzierung über Bundesmittel erheblich erschwert.

Vor diesem Hintergrund sprechen wir uns daher für eine klare Zuständigkeit auf Bundesebene aus bzw. eine bundeseinheitliche Regelung aus. Angesichts der zentralen Bedeutung der Energie- und Wasserinfrastrukturen für das Funktionieren von Wirtschaft, Gesellschaft und Staat ist ein entschlossenes und bundeseinheitliches Handeln hinsichtlich der Drohnenabwehr zwingend erforderlich.

2.2 Verbesserung des Lagebilds: Erarbeitung eines Konzepts zum systematischen Informationsaustausch im Rahmen von Sicherheitspartnerschaften

Aus Sicht der Energie- und Wasserwirtschaft ist festzustellen, dass die Überwachung des unteren Luftraums derzeit nicht auf eine Weise erfolgt, die eine Erstellung systematischer Lagebilder für KRITIS-Betreiber erlauben würde. Es braucht daher ein gemeinsames Zielbild für die Erstellung eines übergreifenden Lagebilds zwischen Sicherheitsbehörden und KRITIS-Betreibern.

In einem ersten Schritt müsste ein flächendeckendes Netzwerk an geeigneter Sensorik zur Drohnenerfassung eingerichtet werden. Zweitens müssten diese gesammelten Daten durch staatliche Stellen gebündelt und ggf. mit Informationen aus der Überwachung des mittleren und höheren Luftraums verbunden werden. In einer entsprechenden Leitstelle sollte diese Informationslage mit den Informationen der KRITIS-Betreiber verschnitten werden. Drittens erfolgt auf Basis der verfügbaren Informationen und eines Data-Fusion-Ansatzes eine Kategorisierung des Flugobjekts und ggf. die Einleitung von Abwehrmaßnahmen.

Wichtig für ein solches Lagebild wäre ein ausreichender Differenzierungsgrad, der es ermöglicht nach unterschiedlichen Spannungsebenen (im Strombereich) zu unterscheiden. Weiterhin sollten Daten zur aktuellen Lage regional differenziert sein, sodass eine möglichst genaue Ableitung der lokalen Gefährdung möglich wird.

Zentral für die Erarbeitung und Umsetzung eines solchen Konzepts sollte dabei eine Sicherheitspartnerschaft zwischen Sicherheitsbehörden und KRITIS-Betreibern sein. In Zeiten der hybriden Bedrohungslage ist der enge Informationsaustausch in beide Richtungen unabdingbar.

Zur Erreichung dieses Zielbilds empfehlen wir daher folgende Maßnahmen:

- › Entwicklung eines Zielbilds für ein gemeinsames Lagebild zur Drohnenabwehr in der kritischen Infrastruktur in Kooperation zwischen Sicherheitsbehörden, BDEW und KRITIS-Betreibern. Hierzu gehören auch die Identifikation und Festlegung von gemeinsamen Prozessen und technischen Schnittstellen.
- › Formalisierung von systematisch aufgebauten Sicherheitspartnerschaften mit dem Ziel des Informationsaustauschs zwischen KRITIS-Betreibern und Sicherheitsbehörden zur Verbesserung des Lagebilds
- › Erprobung und Skalierung von Detektionsprojekten nach Vorbild des [BDEW-Projekts „450detect“](#)
- › Anbindung der KRITIS-Betreiber an das Lagebild des Gemeinsamen Drohnenabwehrzentrums der Bundespolizei (GDAZ), sobald dieses zur Verfügung steht

- › Zugang der KRITIS-Betreiber zu Risikoanalysen bzgl. Drohnen von Bund und Ländern und Bereitstellung über eine effiziente Schnittstelle
- › Vereinfachung und Vereinheitlichung des Meldewegs im Falle einer Drohnensichtung

2.3 Großflächige Flugverbotszonen einrichten und Identifizierungspflicht einführen

Die Bundesregierung hat angekündigt, bis Ende 2026 einen Entwurf für ein Gesetz zur Ausweisung von U-Space-Lufträumen für den optimierten Betrieb von Drohnen (U-Space-Gesetz) vorzulegen. Aus Sicht der Energie- und Wasserwirtschaft kann das U-Space-Gesetz einen wesentlichen Beitrag dazu leisten, eine Bewirtschaftung des unteren Luftraums herzustellen, die die Differenzierung von maliziösen und nicht-maliziösen Drohnen erlaubt. Zum Schutz der kritischen Energie- und Wasserinfrastruktur sollten daher untenstehende Punkte im U-Space-Gesetz priorisiert werden. Alternativ könnte eine Änderung der Luftverkehrs-Ordnung (LuftVO) ebenfalls geeignet sein, um Flugverbotszonen einzurichten.

- (1) Erstens sollten großflächige Flugverbotszonen eingerichtet werden, um das Überfliegen von kritischer Infrastruktur zu reduzieren. Die Flugverbotszonen müssen als räumlich umfassend großzügig genug ausgestaltet werden, um KRITIS-Betreibern bzw. Sicherheitsbehörden eine angemessene Reaktionszeit für Detektion, Einordnung und ggf. Abwehr von Drohnen zu erlauben. Diese Flugverbotszonen müssen ausnahmslos bei allen Herstellern von Drohnen im Sinne eines Geo-Fencing hinterlegt werden. Von größter Bedeutsamkeit ist bei der Einrichtung von Flugverbotszonen, dass diese keine genauen Standorte von kritischen Infrastrukturen offenlegen dürfen und nicht indirekt zu mehr Transparenz zum Nutzen maliziös gesinnter Akteure führen sollten. Weiterhin ist es wichtig, dass Flugverbotszonen so ausgestaltet werden, dass der Drohnen-Einsatz durch KRITIS-Betreiber (oder beauftragte Dienstleister) in bestimmten Flugkorridoren weiterhin möglich bleibt (s. Punkt 2.5).
- (2) Zweitens muss die Identifizierung einzelner Drohnen dringend verbessert werden. Konkret schlagen wir hierfür vor, dass eine echtzeitfähige Remote-ID für alle Drohnenklassen zur Pflicht gemacht wird. Für alle Bestandsdrohnen, auch von Privatpersonen, muss eine Aufrüstungspflicht eingeführt werden. Dies dient vor allem dazu, den privaten Drohnenflug über der kritischen Infrastruktur einzuhegen, der zusätzlich Alarmierungs- und Reaktionsprozesse belastet. Weiterhin ist es zentral, dass die Remote-ID und die damit verbundenen Daten nicht nur den Sicherheitsbehörden zur Verfügung steht, sondern auch über eine geeignete Schnittstelle, den KRITIS-Betreibern zur Erstellung eines Echtzeit-Lagebilds inkl. Kategorisierung von erkannten Drohnenflügen

zugänglich gemacht werden kann. Dabei muss sichergestellt werden, dass diese Daten durch KRITIS-Betreiber bei Bedarf datenschutzkonform genutzt werden.

2.4 Abschreckung unautorisierter nicht-maliziöser Überflüge: Einführung eines Straftatsstands

Unautorisierte Drohnenüberflüge über kritischen Infrastrukturen stellen eine erhebliche Gefahr für die Versorgungs- sowie die Betriebssicherheit dar, sind bislang jedoch nicht spezifisch erfasst. Eine Erweiterung des Strafgesetzbuches, die einen „gefährlichen Eingriff in die kritischen Infrastrukturen der Energie- und Wasserwirtschaft“ normiert, würde eine klare Parallele zu § 315 StGB (Eingriff in den Bahn-, Schiffs- und Luftverkehr) schaffen. Damit würde ein rechtlicher Rahmen etabliert, um solche Eingriffe unmissverständlich zu kriminalisieren und ihre strafrechtliche Verfolgung sicherzustellen. Gleichzeitig muss sichergestellt werden, dass die Abwehr von Drohnen über kritischen Infrastrukturen gemäß § 315 StGB keinen gefährlichen Eingriff in den Luftverkehr und gemäß § 303 StGB keine Sachbeschädigung darstellt.

2.5 KRITIS-Betreibern weiterhin die Nutzung von eigenen Drohnen gestatten

Drohnen erfüllen zugleich schon heute eine wichtige Funktion in der Energie- und Wasserinfrastruktur. Sie werden genutzt, um Anlagen zu inspizieren und z.B. mögliche Schäden frühzeitig und kostensparend zu identifizieren. Drohnen werden seitens der KRITIS-Betriebe für zahlreiche weitere wichtige Aufgaben verwendet, darunter: klassische Leitungsbefliegung, Befliegungen im Rahmen der EU-Methanverordnung, Befliegungen durch Dienstleister im Zuge von Baumaßnahmen oder perspektivisch vermehrt zum Objektschutz. Dadurch tragen Drohnen schon heute zur Versorgungssicherheit bei. Aus den genannten Gründen wäre bei allen Maßnahmen darauf zu achten, dass das Potenzial der Drohnennutzung durch KRITIS-Betreiber nicht beeinträchtigt werden würde.

3 Zusammenfassung

Zusammenfassend empfehlen wir folgende Maßnahmen im Sinne eines Sofortpakets „Drohnenabwehr“. Diese Maßnahmen sollen einen Beitrag zur Erstellung eines gemeinsamen Lagebilds und zur Vereinfachung der Informationslage leisten. Insbesondere die Maßnahmen zur Vereinfachung der Informationslage ließen sich binnen weniger Monate umsetzen.

Gemeinsames Lagebild	Vereinfachung der Informationslage
Erarbeitung eines Konzepts für ein gemeinsames Lagebild im Rahmen von Sicherheitspartnerschaften zwischen Sicherheitsbehörden und KRITIS-Betreibern: › Entwicklung eines gemeinsamen Zielbilds über Prozesse und technische Schnittstellen › Formalisierung von Sicherheitspartnerschaften zw. Sicherheitsbehörden und KRITIS-Betreibern zum kontinuierlichen Informationsaustausch › Anbindung der KRITIS-Betreiber an GDAZ-Lagebild › Zugang zu Risikoanalysen von Bund und Ländern › Vereinfachung und Vereinheitlichung des Meldeweges im Falle einer Drohnensichtung	Zur Vereinfachung der Informationslage sprechen wir uns für folgende Maßnahmen aus: › Flugverbotszonen und Identifizierungspflicht • Einrichtung großflächiger Flugverbotszonen • Einführung einer ausnahmslosen Remote-ID-Pflicht für Drohnen › Abschreckung unautorisierter nicht-maliiziöser Überflüge: Einführung eines Straftatbestands nach §315 StGB › KRITIS-Betreibern weiterhin Drohennutzung gestatten