Berlin, 7. Oktober 2025

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

Positionspapier

Effektive und zukunftssichere Drohnenabwehr für kritische Infrastrukturen: Herausforderungen und gemeinsame Lösungsansätze

Versionsnummer: 1.0

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

Inhalt

1 Executive Summary

1.1 Ausgangslage

Die Zahl unautorisierter Drohnenüberflüge über den kritischen Infrastrukturen in Deutschland nimmt zu. Dabei kann eine Attribuierung zu Personen und deren Absichten durch die Sicherheitsbehörden oder KRITIS-Betreiber praktisch nicht erfolgen. Aufgrund der extrem kurzen Reaktionszeiten und der Risiken, die unautorisierte Drohnen für die kritischen Infrastrukturen sowie die Versorgungssicherheit bergen, ist eine konsequente sowie rechtssichere Behandlung dieser Drohnen erforderlich. Vor diesem Hintergrund fordert der **Bundesverband der Energie- und Wasserwirtschaft (BDEW)** den **Bund** auf, **zügig** die **rechtlichen, technischen und finanziellen Grundlagen für eine wirksame Drohnendetektion** und **-abwehr** zu schaffen. Dies muss der Bund darüber hinaus flankieren mit weiteren **luft-, straf- und telekommunikationsrechtlichen Anpassungen**, damit eine konsequente und rechtssichere Behandlung der zunehmenden Drohnenbedrohung gelingen kann.

Die Abwehr (Störung, Abschuss und Zerstörung) von Drohnen muss dabei eine hoheitliche Aufgabe bleiben. Gleichzeitig kann die Energie- und Wasserwirtschaft mit ihrem Know-how bei der Auswahl geeigneter Lösungen unterstützen, um Fehlentscheidungen und ineffiziente Investitionen zu vermeiden.

1.2 Wesentliche Positionen

Klärung der Zuständigkeiten

- Der Bund muss zeitnah gesetzlich festlegen, welche Behörden für die Drohnenabwehr verantwortlich sind und welche Mitwirkungspflichten die Energie- und Wasserwirtschaft hat.
- Betreiber kritischer Infrastrukturen dürfen nicht verpflichtet werden, eigenständig Systeme zur Drohnenabwehr zu beschaffen und zu betreiben.

Option einer Beleihung im Ausnahmefall

- Wenn vorbeugende Maßnahmen oder Business Continuity Management (BCM) nicht ausreichen und staatliche Kapazitäten fehlen, sollte eine **Beleihung von Betreibern unter klaren gesetzlichen Rahmenbedingungen und auf Ersuchen der KRITIS-Betreiber** ermöglicht werden. **So bliebe das staatliche Gewaltmonopol gewahrt.**

Notwendige Anpassungen im Luftsicherheits-, Straf- und Telekommunikationsrecht

- **Flugverbotszonen und U-Spaces:** Zügige Einrichtung von Flugverbotszonen über kritischen Infrastrukturen sowie Integration dieser in U-Spaces zur geordneten Drohnenbewirtschaftung im unteren Luftraum.

- **Strafrechtliche Anpassung:** Einführung eines Straftatbestandes im StGB, der unautorisierte Drohnenüberflüge als „gefährlichen Eingriff in die kritischen Infrastrukturen der Energie- und Wasserwirtschaft“ analog zu § 315 StGB erfasst. Gleichzeitig muss sichergestellt werden, dass die Abwehr von Drohnen über kritischen Infrastrukturen selbst keine Straftat darstellt.
- **Einsatz von elektromagnetischen Wirkmitteln:** Anpassung des Telekommunikationsgesetzes i. V. m. § 317 StGB, um beliehenen KRITIS-Betreibern die rechtliche Möglichkeit zum Einsatz von elektromagnetischen Wirkmitteln einzuräumen.
- **Weitere Schutztechnologien:** Schaffung unbürokratischer und pragmatischer Voraussetzungen durch die Bundesnetzagentur für die Erprobung und den Einsatz neuartiger elektromagnetischer Wirkmittel (z. B. High-Power-Microwave-Systeme).

Finanzierung sicherstellen

- **Investitionen in Prävention, Detektion und Abwehr** müssen als **betriebsnotwendige Aufwendungen** anerkannt werden und eine **Refinanzierung** über **Entgelte** und **Gebühren** möglich sein.
- Darüber hinaus ist eine **staatliche Mitfinanzierung – auch aus dem Verteidigungshaushalt – erforderlich**, da die Infrastrukturen essenziell für Bevölkerung, Bundeswehr und NATO sind.

Anpassung der Transparenzpflichten

- **Offen verfügbare Leistungs- und Geodaten kritischer Infrastrukturen** erhöhen die Verwundbarkeit der kritischen Infrastrukturen.
- **Transparenzpflichten** müssen daher **neu bewertet**, **eingeschränkt** und **abstrahiert** werden.

Mangelnde Marktverfügbarkeit geeigneter Lösungen

- **Marktverfügbare Lösungen** sind **zur flächendeckenden Abwehr** nicht-kooperativer / autonomer Drohnen und Drohnenschwärmen **nicht vollumfänglich geeignet**.

Lösungsansätze

- **Rechtssichere Beleihungsmodelle** mit klaren Regelungen zur Haftungsfreistellung der KRITIS-Betreiber und Haftungsübernahme seitens des Staats.
- **Zügige Anpassungen im Luftsicherheits-, Straf- und Telekommunikationsrecht.**
- **Reallabore** von Bund, Ländern, Sicherheitsbehörden, Bundeswehr und Betreibern zur praxisnahen Erprobung von Technologien.

- **Standardisierte Schnittstellen und Datenfusion**, um ein bundesweites, behörden- und betreiberübergreifendes Lagebild zu schaffen.

2 Ausgangslage und wesentliche Positionen

Die Zunahme von unautorisierten Drohnenüberflügen über unseren kritischen Infrastrukturen zeigt, dass der **Bund zügig die rechtlichen, technischen und finanziellen Voraussetzungen für eine wirksame Drohnendetektion und -abwehr durch die Sicherheitsbehörden von Bund und Ländern schaffen muss**. Hierdurch muss eine rechtssichere Behandlung der zunehmenden unautorisierten Drohnenüberflüge möglich sein. **Dabei muss aus Sicht des Bundesverbandes der Energie- und Wasserwirtschaft (BDEW) die Abwehr (insbesondere Störung, Abschuss und Zerstörung) von Drohnen hoheitliche Aufgabe bleiben.**

Die **Energie- und Wasserwirtschaft** verfügt aber über **fundierte Kenntnisse der spezifischen Herausforderungen bei der Absicherung kritischer Infrastrukturen in den Bereichen Energie, Wasser und Abwasser**. Mit dieser Expertise kann die **Energie- und Wasserwirtschaft** den **Bund** bei der **Identifizierung geeigneter Lösungsansätze** – wie etwa des aus ihrer Mitte entwickelten **LTE450-Passivradars zur Drohnendetektion** – wirkungsvoll unterstützen. Auf diese Weise soll auch verhindert werden, dass für den Schutz kritischer Infrastrukturen ungeeignete Systeme beschafft und Fehlinvestitionen getätigt werden. **Denn aus Sicht des BDEW sind die zurzeit marktverfügbaren Lösungen zur Detektion und Abwehr von Drohnen in der Fläche nicht vollumfänglich geeignet.** Zudem kommen neben der Drohnenabwehr noch andere Mittel zur Behandlung der Drohnenbedrohung infrage: Auch vorbeugende Sicherheitsmaßnahmen oder Maßnahmen des Business Continuity Managements können einen wichtigen Beitrag leisten, um den Schutz und die Resilienz der kritischen Infrastrukturen gegenüber Drohnen zu stärken.

Mit diesem Positionspapier möchte der BDEW einen ersten Impuls zu gemeinsamen Lösungsansätzen für eine effektive und zukunftssichere Drohnenabwehr für kritische Infrastrukturen geben. Wesentliche Positionen des Positionspapiers sind dabei:

1. **Zügige gesetzliche Klärung** über die **Zuständigkeiten bei der hoheitlichen Aufgabe Drohnenabwehr** sowie der Mitwirkungspflichten der Energie- und Wasserwirtschaft. **Daraus darf sich keine gesetzliche Verpflichtung für die Betreiber kritischer Infrastrukturen zur Beschaffung und zum Betrieb von Systemen zur Drohnenabwehr ergeben.** Jedoch ist eine enge Einbeziehung der Betreiber notwendig. Allein die KRITIS-Betreiber können im Rahmen einer risikobasierten Bewertung der Schutzbedarfe die

effektiven, verhältnismäßigen und wirtschaftlichen Maßnahmen für ihre kritischen Infrastrukturen identifizieren und die Abwägung zwischen vorbeugenden Sicherheitsmaßnahmen, physischen Schutzmaßnahmen oder Maßnahmen des Business Continuity Managements (BCM) vornehmen.

2. Wenn aber aus Sicht der KRITIS-Betreiber in Einzelfällen weder vorbeugende Sicherheitsmaßnahmen noch physische Schutzmaßnahmen oder Maßnahmen des Business Continuity Managements (BCM) hinreichend zur Risikobehandlung geeignet sind und eine Fähigkeitslücke bei der Drohnenabwehr auf den Seiten der Sicherheitsbehörden besteht, **könnte auf Ersuchen der KRITIS-Betreiber eine Beleihung zur Übernahme der hoheitlichen Aufgabe Drohnenabwehr in Erwägung gezogen werden.** Durch eine Beleihung bliebe das **staatliche Gewaltmonopol gewahrt**, da die Betreiber nicht eigenständig hoheitlich handeln, sondern im Auftrag und im Rahmen klar definierter Befugnisse agieren.

3. Weitere Anpassungen im Luftsicherheits-, Straf- und Telekommunikationsrecht sind für eine effektive Drohnenabwehr erforderlich. Neben der zügigen **Einrichtung von Flugverbotszonen oder Flugbeschränkungsgebieten** über den kritischen Infrastrukturen und der **Einbindung der kritischen Infrastrukturen in U-Spaces zur Drohnenbewirtschaftung** im unteren Luftraum **sollten unautorisierte Drohnenüberflüge zukünftig als strafbare Eingriffe in die kritischen Infrastrukturen der Energie- und Wasserwirtschaft** behandelt werden. Dazu sollte eine Regelung im Strafgesetzbuch geschaffen werden, die analog zum gefährlichen Eingriff in den Bahnverkehr den **gefährlichen Eingriff in die kritischen Infrastrukturen der Energie- und Wasserwirtschaft** unter Strafe stellt. 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. Darüber hinaus muss das **Telekommunikationsgesetz in Verbindung mit dem § 317 Strafgesetzbuch** geändert werden, **damit beliehene KRITIS-Betreiber elektromagnetische Wirkmittel zum Einsatz bringen dürfen**. Schließlich muss die Bundesnetzagentur für die Einführung neuartiger elektromagnetischer Wirkmittel (z.B. High-Power-Microwave-Systeme), die für den Schutz der kritischen Infrastrukturen gegen Drohnen geeignet sind, die unbürokratischen und pragmatischen Voraussetzungen für die Erprobung und den Einsatz schaffen.

4. Mit Blick auf die **hybride Lage und eine resiliente Gesamtverteidigung** müssen für die **Energie- und Wasserwirtschaft geeignete Regelungen und Voraussetzungen für die Finanzierung von vorbeugenden Sicherheitsmaßnahmen oder Systemen zur Detektion und Abwehr von Drohnen inklusive einer staatlichen Finanzierung im Rahmen des Verteidigungshaushaltes** geschaffen werden. Die Infrastrukturen der Energie- und Wasserversorgung sind für die Bundeswehr und ihre Verbündeten im Rahmen des OPLAN Deutschland sowie für die Produktion der Sicherheits- und Verteidigungsindustrie essenziell.

5. **KI-basierte Suchmaschinen oder Algorithmen** ermöglichen das systematische Sammeln, Aufbereiten und Zweckentfremden von Informationen aus dem Internet. So können beispielsweise **potenzielle Angriffsziele identifiziert** und **autonome Drohnen programmiert** werden. **Vor diesem Hintergrund müssen die Transparenzpflichten für Betreiber kritischer Infrastrukturen zügig und ganzheitlich neu bewertet und angepasst werden.** Bestehende Webangebote, die systematisch Leistungsdaten und / oder Geolokationen von kritischer Infrastruktur bereitstellen, müssen beschränkt / abstrahiert werden.

3 Herausforderungen der effektiven Drohnenabwehr bei kritischen Infrastrukturen in der Fläche

Der Krieg in der Ukraine zeigt, dass eine **effektive Luftabwehr bei Versorgungsinfrastrukturen auch gegenüber kleineren, nicht-kooperativen und zunehmend autonom operierenden Drohnen** für die Resilienz und Verteidigungsfähigkeit entscheidend sein wird. Insbesondere die Infrastrukturen der Energie- und Wasserversorgung und Abwasserentsorgung sind für die Bundeswehr und ihre Verbündeten im Rahmen des OPLAN Deutschland sowie für die Produktion der Sicherheits- und Verteidigungsindustrie essenziell.

Im Gegensatz zu kooperativen Drohnen, die einen Kommunikationslink zwischen Angreifer und Drohne benötigen, um ins Ziel zu gelangen, benötigen **nicht-kooperative Drohnen keinen Kommunikationslink**. **Dadurch sind sie deutlich schwieriger aufzuklären und abzuwehren**.

Eine Besonderheit stellen Glasfaser-gelenkte Drohnen dar: Diese verfügen zwar einerseits über einen Kommunikationslink. Dieser kann andererseits aber nicht durch Störsender (Jammer) unterbrochen werden. Eine Unterbrechung des Kommunikationslinks dieser Drohnen gelingt zurzeit lediglich auf mechanischem Wege (Durchtrennung der Glasfaserleitung). Die

Entwicklung Glasfaser-gelenkter Drohnen wurde in der Ukraine notwendig, weil der Einsatz funkgeleiteter Drohnen aufgrund der Sättigung des elektromagnetischen Spektrums durch hochwirksame Lösungen der sogenannten elektronischen Kampfführung zunehmend erschwert wurde. Glasfaser-gelenkte Drohnen bieten gegenüber nicht-kooperativen Drohnen, die autonom operieren, den Vorteil, dass ein Angreifer jederzeit Einfluss nehmen kann auf das Flugverhalten, selbst in einem elektromagnetisch übersättigten Einsatzgebiet. Allerdings erlaubt die Führung der Drohne über Lichtwellenleiter grundsätzlich auch eine Rückverfolgung zur Startplattform.

Der **Trend zum Einsatz nicht-kooperativer Drohnen** scheint zudem auch **in Deutschland angekommen** zu sein. Dies kann durch die Erfahrungen der Betreiber kritischer Infrastrukturen hierzulande gestützt werden: **Illegale Drohnenüberflüge lassen sich durch die am Markt verfügbaren Lösungen – insbesondere durch Funkpeilung – zunehmend nicht mehr aufklären.** Dabei wird die Funkpeilung aber nicht nur durch den Einsatz von nicht-kooperativen Drohnen erschwert, sondern auch durch die korrekte Kalibrierung der Funkpeiler. Die effektive Funkpeilung verlangt die konstanten Anpassungen an die Updates und Einstellungen der Drohnenhersteller. Das setzt auch die größtmögliche Transparenz der Drohnenhersteller und Kooperationsbereitschaft dieser Hersteller gegenüber den Anbietern von Lösungen zur Funkpeilung voraus. Beides lässt sich vor dem Hintergrund der aktuellen geopolitischen Spannungen nicht mehr uneingeschränkt voraussetzen.

Der Trend zu nicht-kooperativen Drohnen hat erhebliche Auswirkungen auf die Auswahl und Marktverfügbarkeiten geeigneter Sensorik zur Detektion und Effektorik zur Abwehr von Drohnen. Für den zivilen Einsatz geeignete Detektions-Lösungen nutzen vorwiegend Funkpeilung. Gleiches gilt für die Abwehr von nicht-kooperative Drohnen durch Störsender (Jammer). Störsender wirken auf den Kommunikationslink von kooperativen Drohnen so ein, dass deren gesteuerter Einsatz nicht mehr möglich ist. Entfällt der Kommunikationslink, ist ein effektiver Einsatz von Störsendern auch nicht mehr möglich.

Es ist davon auszugehen, dass **nicht-kooperative / autonome Drohnen und Drohnenschwärme als günstige Angriffsplattformen bei hybriden oder offen ausgetragenen militärischen Operationen gegen das stark dezentralisierte Energiesystem in Deutschland zum Einsatz** kommen könnten. Die Verfügbarkeit von Leistungs- und Geodaten der kritischen Infrastrukturen über maschinell auslesbare Online-Ressourcen stellt für dieses Szenario einen begünstigenden Faktor dar.

Folgende Faktoren sind darüber hinaus für Einsatzszenarien von autonomen und / oder nicht-kooperativen Drohnen gegen kritische Infrastrukturen begünstigend:

- Das Fehlen einer Funkverbindung erschwert eine Rückverfolgung und Attribuierung erheblich.
- Wirtschaftlichkeit und Verfügbarkeit großer Stückzahlen gegenüber konventionellen militärischen Wirkmitteln.
- Hohe Reichweiten sowie Automatisierung erlauben weitreichende und koordinierte Angriffe.
- Möglichkeit des unauffälligen Einsatzes z.B. über Container-Lösung auf zivilen LKW- / PKW-Plattformen aus dem Bundesgebiet heraus.

Vor diesem Hintergrund sind aus Sicht des BDEW die am Markt verfügbaren Lösungen zur Detektion und Abwehr von Drohnen zurzeit nicht für eine effektive und zukunftssichere Drohnenabwehr für die kritischen Infrastrukturen in der Fläche sowie gegenüber zunehmend nicht-kooperativen / autonomen Drohnentypen vollumfänglich geeignet. Weder können diese Lösungen neue Drohnentypen durch Funkpeilung detektieren noch durch Störsender abwehren.

Bei vielen **Millionen Kilometern an leitungsgebundenen Infrastrukturen** zu Land und zur See sowie den damit verbundenen Energieanlagen können **weder Behörden noch die Betreiber selbst jederzeit vor Ort** sein. Daraus ergibt sich die Notwendigkeit eines hohen **Automatisierungs- und Vernetzungsgrads**, um eine **effektive Drohnenabwehr in der Fläche** zu gewährleisten.

Damit **Investitionen von Staat und Wirtschaft in Technologien zur Detektion und Abwehr von Drohnen zukunftssicher erfolgen** und **keine Fehlinvestitionen** durch die Beschaffung bereits heute nur eingeschränkt geeigneter Systeme entstehen, ist eine **zügige und gemeinsame Lösungsbeschreibung durch Bund, die für die Drohnenabwehr zuständigen Sicherheitsbehörden, die Bundeswehr sowie die Energie- und Wasserwirtschaft und andere KRITIS-Sektoren erforderlich**.

Darüber hinaus müssen sich die KRITIS-Betreiber verstärkt in die Lage versetzen, nach erfolgreichen Angriffen Inselnetze stabil zu betreiben und beschädigte Infrastruktur schnell wieder instand zu setzen. Die dafür entstehenden Mehrkosten sind vom Staat zu bezuschussen oder im Rahmen von Kostenprüfungen für Netzentgelte anzuerkennen.

4 Anpassungsbedarfe des rechtlichen Rahmens

4.1 Zügige Klärung der Zuständigkeit und Möglichkeit zur Beleihung der Betreiber

Die aktuelle Rechtslage in Deutschland weist erhebliche Zuständigkeits- und Befugnisgrenzen bei der Drohnenabwehr auf, die eine wirksame Verteidigung kritischer Infrastrukturen in der Fläche erschweren.

Während die **Bundeswehr im Verteidigungsfall** über den vollen Zugriff auf militärische Wirkmittel verfügt, ist ihr Einsatz im Inland und in Friedenszeiten verfassungsrechtlich stark begrenzt.

Bundes- und Landespolizeien sind zuständig für die Gefahrenabwehr im zivilen Luftraum, haben jedoch bislang nur eingeschränkten Zugriff auf geeignete Effektorik wie Jammer oder begrenzte kinetische Mittel wie Fangnetzdrohnen.

Die **Bundesnetzagentur** reguliert und vergibt Frequenzen und ist für die Zulassung von Störsendern verantwortlich, was für zivile Betreiber bislang de facto den Ausschluss von wirksamer technischer Abwehr bedeutet.

KRITIS-Betreiber selbst dürfen derzeit ausschließlich präventive und organisatorische Maßnahmen wie Geo-Fencing oder physische Barrieren ergreifen. Diese Maßnahmen können zusammen mit Maßnahmen des Business Continuity Managements oftmals ausreichend sein, um die Infrastrukturen gegenüber Drohnen zu schützen oder resilienter zu machen. Zudem kann durch das (n-1)-Kriterium in bei vielen kritischen Infrastrukturen der Ausfall eines Betriebsmittels im Zuge eines Drohnenangriffs im Grundsatz durch ein anderes Betriebsmittel kompensiert werden. Gleichwohl kann sich für die Betreiber kritischer Infrastrukturen der zusätzliche Bedarf für Systeme zur Drohnenabwehr ergeben. In diesem Fall ist die beschriebene Zuständigkeitsverteilung der Herausforderung nicht mehr gewachsen. Weder die Polizei noch andere staatliche Stellen können bei Millionen Kilometern leitungsgebundener Infrastrukturen eine durchgehende Präsenz gewährleisten.

KRITIS-Betreiber könnten in diesem Fall allerdings durch ein **Beleihungsmodell** befugt werden, unter strengen Auflagen und staatlicher Aufsicht **bestimmte Formen der Effektorik** – etwa Jammer, Abfangdrohnen ohne Sprengköpfe, High-Power-Microwave-Systeme (HPM) oder Lasersysteme mit kurzer Reichweite und hochpräziser Strahlschwenkung – einzusetzen.

Die Beleihung ist im deutschen Verwaltungsrecht eines von mehreren Instrumenten zur Übertragung bestimmter hoheitlicher Aufgaben auf juristische Personen des Privatrechts unter staatlicher Aufsicht (Rechts- und Fachaufsicht). Eine Beleihung setzt die Übertragung einer

konkreten hoheitlichen Aufgabe oder Befugnis durch oder aufgrund eines Gesetzes voraus. Es braucht also eine explizite gesetzliche Grundlage, die beschränkt ist auf eine spezielle Zuständigkeit. Vergleichbare Modelle existieren bereits in der Luftsicherheit: So eröffnet § 16a Luftsicherheitsgesetz (LuftSiG) die Möglichkeit, Aufgaben des Sicherheitsbereichs an private Luftsicherheitsunternehmen zu übertragen, die dann unter hoheitlicher Aufsicht tätig werden. Eine Beleihung ermöglicht auch die Ausübung hoheitlicher Gewalt.

Nur so lässt sich eine schnelle, flächendeckende und zugleich verantwortbare Drohnenabwehr für kritische Infrastrukturen in Deutschland sicherstellen.

Ein zentraler Baustein für eine Beleihung sind dabei **vordefinierte Sicherheitsgrenzen**. Dazu gehört insbesondere die **Einrichtung verbindlicher Flugverbotszonen** über KRITIS-Anlagen, die in U-Space-Systeme integriert und durch Geo-Fencing in allen marktüblichen Drohnensystemen technisch abgebildet werden müssen. Damit wäre rechtlich klargestellt, dass jede nicht autorisierte Drohne in diesem Bereich unzulässig ist und automatisierte Abwehrmaßnahmen gegen solche Ziele legitim ausgelöst werden könnten. Weitere Sicherheitsgrenzen betreffen die **eindeutige Zielidentifikation durch Sensorfusion**, die **räumliche Eingrenzung des Abwehrbereichs**, die **Beschränkung auf verhältnismäßige Wirkmittel** sowie die Verpflichtung zu **Fail-Safe-Mechanismen** und **lückenloser Protokollierung** aller Maßnahmen.

Mit einer Beleihung der KRITIS-Betreiber durch den Staat stellt sich zugleich die Frage nach **Haftung und Versicherbarkeit**. Derzeit riskieren Betreiber zivilrechtliche Haftungsansprüche von Dritten, wenn Abwehrmaßnahmen unzulässig oder fehlerhaft ausgelöst werden.

Beliehene haften hingegen nach außen nicht selbst, vielmehr findet eine Haftungsüberleitung auf den Staat statt. Geschädigte müssen ihre Ansprüche nach den Grundsätzen der **Amtshaftung nach Art. 34 Grundgesetz (GG) in Verbindung mit § 839 BGB geltend machen**.

Es stellt sich aber die Frage nach den Rückgriffsmöglichkeiten des Staates gegenüber dem Beliehenen. Das Haftungsprivileg von Beamten (Artikel 34 Satz 2 GG: Rückgriff nur bei Vorsatz oder grober Fahrlässigkeit) greift nicht. **Deshalb braucht es eine entsprechende Freistellung im Gesetz oder Vertrag.**

Für die Betreiber kritischer Infrastrukturen ermöglicht dies, dass sie im Rahmen einer Beleihung rechtssicher agieren könnten, ohne unkalkulierbare persönliche oder unternehmerische Haftungsrisiken tragen zu müssen. Damit würde zugleich die **Versicherbarkeit des Einsatzes von Drohnenabwehrsystemen** gewährleistet und die notwendige Planungssicherheit geschaffen, ohne das staatliche Gewaltmonopol in Frage zu stellen.

4.2 Notwendige Anpassungen im Luftsicherheits-, Straf- und Telekommunikationsrecht

Für eine wirksame Drohnenabwehr im Bereich der kritischen Infrastrukturen sind umfassende Anpassungen im Luftsicherheits-, Straf- und Telekommunikationsrecht erforderlich.

Derzeit nehmen unautorisierte Drohnenüberflüge über Anlagen der Energie- und Wasserversorgung kontinuierlich zu. Zwar existieren punktuelle Flugverbotszonen, deren Einrichtung erfolgt jedoch bislang fragmentiert und mit erheblichem Zeitaufwand. **Eine flächendeckende, zügige und rechtlich verbindliche Absicherung kritischer Infrastrukturen durch klar definierte Flugverbotszonen ist daher dringend geboten.** Ergänzend hierzu werden U-Spaces in Deutschland schrittweise eingeführt, um den unteren Luftraum strukturiert zu bewirtschaften und sichere Drohnenoperationen zu gewährleisten. Damit diese Regelungen ihre Schutzwirkung entfalten können, ist es notwendig, kritische Infrastrukturen systematisch in die U-Spaces einzubinden und so unautorisierte Überflüge von vornherein zu unterbinden.

Unabhängig von einer Beleihung gemäß 4.1 sollte es KRITIS-Betreibern grundsätzlich erlaubt werden, selbst autonome Drohnen zur Überwachung eigener Anlagen (Aufklärung und Detektion) einzusetzen.

Neben der Regulierung des Luftraums bedarf es einer Weiterentwicklung des Strafrechts. Unautorisierte Drohnenüberflüge über kritischen Infrastrukturen stellen eine erhebliche Gefahr für die Versorgungssicherheit 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 Bahnverkehr) 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.

Darüber hinaus muss das Telekommunikationsrecht an die sicherheitspolitischen Erfordernisse angepasst werden. Nach derzeitiger Rechtslage sind KRITIS-Betreiber nicht befugt, Störsender einzusetzen, da das Telekommunikationsgesetz in Verbindung mit § 317 StGB deren Nutzung ausschließt. Um unmittelbare Gefahrenlagen vor Ort wirksam bewältigen zu können, ist eine gesetzliche Öffnung erforderlich, die den Einsatz von elektromagnetischen Wirkmitteln durch Betreiber kritischer Infrastrukturen ausdrücklich erlaubt.

Schließlich ist auch der Einsatz innovativer Schutztechnologien in den Blick zu nehmen. Neuartige elektromagnetische Wirkmittel wie HPM-Systeme könnten einen wirksamen Beitrag zur Drohnenabwehr leisten. Hierfür sollte die Bundesnetzagentur pragmatische und unbürokratische Voraussetzungen schaffen, die eine zeitnahe Erprobung und einen geregelten

Einsatz dieser Technologien ermöglichen. Nur durch das abgestimmte Zusammenspiel von Luftraumregulierung, strafrechtlicher Sanktionierung und technologischen Abwehrmaßnahmen lässt sich ein wirksamer Schutz der kritischen Infrastrukturen gegen die zunehmenden Gefahren durch unautorisierte Drohnennutzung gewährleisten.

4.3 Finanzierung, Kostenanerkennung, Entgelt- bzw. und Gebührenfähigkeit

Für eine wirksame Resilienz der Energie- und Wasserwirtschaft sowie eine fortgesetzte Wettbewerbsfähigkeit des Energiestandorts Deutschlands in Europa ist zunächst sicherzustellen, dass Investitionen in neue Schutzsysteme **als betriebsnotwendige Aufwendungen anerkannt** und damit über die **Entgelte und Gebühren refinanzierbar** sind. Erforderlich ist auch eine eindeutige **Regelung zur Kostenanerkennung durch die Bundesnetzagentur**. Nur so können Betreiber kritischer Infrastrukturen mit Planungssicherheit investieren und gleichzeitig sicherstellen, dass die Refinanzierung im Rahmen der regulierten Entgeltsysteme gewährleistet ist. **Darüber hinaus muss die Finanzierung der Systeme durch den Staat insbesondere in nicht-regulierten Bereichen der Energiewirtschaft (d.h. Betreiber kritischer Energieanlagen) flankiert werden.**

Angesichts der zunehmenden hybriden Bedrohungslage ist es erforderlich, dass Drohnenabwehrmaßnahmen der Energie- und Wasserwirtschaft auch aus dem **Verteidigungshaushalt** gestützt werden. Hierbei ist der strategische Kontext der NATO maßgeblich: Mit der Beschlusslage zur **5 Prozent-Verteidigungsverpflichtung bis 2035**, von der bis zu **1,5 Prozent des BIP für Resilienzmaßnahmen** vorgesehen sind, eröffnen sich neue Finanzierungsräume. Systeme zur Drohnendetektion und -abwehr für kritische Infrastrukturen fallen aus unserer Sicht unmittelbar in diesen Resilienztatbestand. Ihre Förderung ist daher sowohl national als auch europäisch und transatlantisch als Bestandteil der Gesamtverteidigung zu verankern.

Die **Infrastrukturen der Energie- und Wasserwirtschaft** sind nicht nur für die Bevölkerung unverzichtbar, sondern auch für die **Operationsfähigkeit der Bundeswehr und ihrer Verbündeten im Rahmen des Host Nation Supports bzw. des OPLAN Deutschland** sowie für die Funktionsfähigkeit der Sicherheits- und Verteidigungsindustrie. Entsprechend muss die Kostenanerkennung durch die Bundesnetzagentur Hand in Hand mit der staatlichen Mitfinanzierung erfolgen, um sowohl die betriebliche Tragfähigkeit als auch die nationale und bündnisstrategische Resilienz sicherzustellen.

Für Deutschland bedeutet dies: Die energie- und wasserspezifische Resilienz ließe sich künftig national wie bündnisstrategisch finanzieren. Neue Schutzsysteme wie Systeme zur Detektion und Abwehr von Drohnen sollten als legitime Resilienzinvestitionen gelten, für die

entsprechende Förderkulissen im Verteidigungshaushalt geschaffen werden müssen – im Sinne einer wirksamen **Gesamtverteidigung**, die zivile Infrastrukturen schützt und damit auch die Verteidigungsfähigkeit sichert.

4.4 Neubewertung von Transparenzpflichten

Die Verfügbarkeit von Leistungs- und Geodaten kritischer Infrastrukturen über maschinell auslesbare Online-Ressourcen von Behörden, kommunalen Einrichtungen, aber auch von Web-Serviceanbietern oder Open-Source-Quellen begünstigt Einsatzszenarien von nicht-kooperativen und autonomen Drohnen gegen kritische Infrastrukturen. Mit den verfügbaren Plattformen und Tools für Open Source Intelligence (OSINT) lassen sich mit relativ geringem Aufwand direkte Zuordnungen von Bildquellen, Geokoordinaten (UMT & GPS) und kritischen Infrastrukturen herstellen. **In diesem Zusammenhang müssen auch die rechtlichen Rahmenbedingungen bei den Transparenzpflichten für Betreiber und Aufsichtsbehörden kritischer Infrastrukturen zügig und ganzheitlich neu bewertet und angepasst werden.** Bestehende Webangebote von Behörden oder von Open-Source-Quellen, die systematisch Leistungsdaten und / oder Geolokationen von kritischer Infrastruktur bereitstellen, sollten deshalb beschränkt / abstrahiert werden.

Es sollte in Zukunft bei Portalen von Behörden und Einrichtungen auf Bundes- und Landesebene sowie der Kommunen grundsätzlich nachvollziehbar sein, wer Infrastrukturdaten abruft. Auch sollten deshalb Ausschreibungen und Verbändebeteiligungen in Zukunft nur der Branche und Stakeholdern mit nachgewiesenem Interesse, nicht aber einer breiten Öffentlichkeit zugänglich gemacht werden, wenn diese sicherheitsrelevante Aspekte der Planung und Umsetzung von Vorhaben der kritischen Infrastrukturen zum Inhalt haben.

Schließlich sollten die möglichen Risiken von Transparenzpflichten für die kritischen Infrastrukturen im Rahmen der Nationalen Risikoanalyse gemäß CER-Richtlinie betrachtet werden.

4.5 Automatisierte Drohnenabwehrsysteme mit vordefinierten Sicherheitsgrenzen

Die Erfahrungen aus aktuellen Konflikten zeigen, dass Drohnenangriffe – insbesondere durch Schwärme oder hochgradig autonome Systeme – mit extrem kurzen Vorwarn- und Reaktionszeiten erfolgen können. Unter diesen Bedingungen ist eine rein menschliche Reaktionskette regelmäßig nicht in der Lage, die notwendige Abwehrgeschwindigkeit sicherzustellen. Für den Schutz kritischer Infrastrukturen in der Fläche ergibt sich hieraus die Notwendigkeit, **automatisierte Systeme** einzusetzen, **die in bestimmten Szenarien und beim Vorliegen einer besonders schweren Bedrohungslage unmittelbar reagieren können**.

Dabei ist das **Selbstschutzprinzip** (Notwehr / Nothilfe) leitend: Behörden oder KRITIS-Betreiber dürfen mit Blick auf zukünftige Szenarien nicht in die Position gebracht werden, dass Angreifer über automatisierte Drohnentechnologie verfügen, während der Schutz kritischer Infrastrukturen an menschlichen Reaktionsgrenzen scheitert. Automatisierte Abwehrhandlungen sind aus Sicht des BDEW daher dann legitim, wenn sie **innerhalb enger, vordefinierter Sicherheitsgrenzen** erfolgen.

Diese Sicherheitsgrenzen könnten folgende Kriterien umfassen:

- **Geographische Eingrenzung:** Automatisierte Maßnahmen dürfen ausschließlich im definierten Schutzbereich, der zugleich als Flugverbotszone gekennzeichnet ist, ausgelöst werden.
- **Eindeutige Zielidentifikation:** Der Einsatz darf nur erfolgen, wenn durch mehrschichtige Sensorfusion zweifelsfrei ein unautorisiertes Luftfahrzeug in einer festgelegten Flugverbotszone erkannt wird.
- **Wirkmittelbeschränkung:** Automatisierte Systeme dürfen nur verhältnismäßige, risikoarme Effekte auslösen. Kinetische Effektoren mit Sprengwirkung sollten staatlichen Eingriffsbefugnissen vorbehalten bleiben.
- **Fail-Safe-Mechanismen:** Systeme müssen jederzeit abschaltbar sein und sich bei Fehlfunktion automatisch in einen sicheren Zustand versetzen.
- **Transparenz und Nachvollziehbarkeit:** Jede automatisierte Entscheidung ist revisionssicher zu protokollieren und der Aufsicht der zuständigen Sicherheitsbehörden zugänglich zu machen.

Nur durch die **Kombination aus automatisierter Reaktionsfähigkeit und klar definierten Sicherheitsgrenzen** kann einerseits der notwendige Schutz kritischer Infrastrukturen in der Fläche gewährleistet werden, während andererseits die Grundprinzipien menschlicher Kontrolle und Verantwortbarkeit gewahrt bleiben.

5 Gemeinsame Lösungsansätze

5.1 Schaffung gemeinsamer Reallabore

Zur zügigen, praxistauglichen Einführung wirksamer Drohnenabwehr für kritische Infrastrukturen braucht es **gemeinsame Reallabore** von Bund, Ländern, zuständigen Sicherheitsbehörden, Bundeswehr, Fachaufsichten (u. a. Bundesnetzagentur, Deutsche Flugsicherung), der Forschung sowie Energie- und Wasserwirtschaft. Dabei sollte es nicht nur

um die gemeinsame Identifizierung und Erprobung geeigneter Lösungen gehen, sondern auch um das gemeinsame und praxisnahe Üben des Einsatzes solcher Systeme in verteilten Aufgaben- und Zuständigkeitsrollen.

Das derzeit im Gesetzgebungsverfahren befindliche **Reallabore-Gesetz** schafft dafür einen einheitlicheren, innovationsfreundlichen Genehmigungsrahmen und adressiert typische Hürden wie Definitionen, Verfahren und Wissenstransfer; diese Struktur sollte gezielt für Pilotprojekte zum Schutz kritischer Infrastrukturen genutzt werden.

Parallel verpflichtet die **EU-KI-Verordnung** die Mitgliedstaaten zur Einrichtung **regulatorischer KI-Sandboxes**. In diesen geschützten Umgebungen können Hochrisiko-KI-Systeme – etwa multisensorische Detektions- und Entscheidungsunterstützung für Drohnenabwehr – datenschutzkonform, mit menschlicher Aufsicht und Audit-Pflichten getestet und zur Konformität geführt werden. Diese Sandboxes sollten mit nationalen Reallaboren gekoppelt und für KRITIS-Anwendungen geöffnet werden.

Für die **Luftraum-Einbindung** empfiehlt sich, Reallabore testweise in **U-Space-Gebieten** zu verorten, um digitale Flugverbotszonen, Geo-Fencing, Melde- und Freigabeprozesse sowie Schnittstellen zu Deutscher Flugsicherung und Sicherheitsbehörden realitätsnah zu erproben.

Flankierend stehen **Förderkulissen** auf Bundesebene bereit – insbesondere das Rahmenprogramm „Forschung für die zivile Sicherheit 2024–2029“ mit Demonstrations- und Erprobungsvorhaben –, die als finanzielle Träger für KRITIS-Reallabore genutzt und gezielt auf Drohnenabwehr ausgerichtet werden sollten.

5.2 Spezifische Schnittstellen und Datenfusion zur umfassenden Lagebilderstellung

Geeignete Schnittstellen und Protokolle für die Integration geeigneter Sensorik und Effektorik müssen zeitnah identifiziert und ggf. weiterentwickelt werden, um ein hohes Maß an Standardisierung, Interoperabilität, Skalierung und Offenheit für die Weiterentwicklung zu erzielen. Dadurch können die Wirtschaftlichkeit und Zukunftsoffenheit bei der anstehenden Beschaffung erhöht werden.

Es sollten dabei marktverfügbare bzw. schon im Einsatz befindliche Systeme und digitale Infrastrukturen genutzt werden, wenn diese eine schnelle Integration geeigneter Sensorik und Effektorik ermöglichen. **Ziel sollte es sein, die Voraussetzung für ein bundesweites Lagebild zu schaffen, auf das Behörden, Bundeswehr und KRITIS-Betreiber gleichermaßen zurückgreifen können. Dabei sollte das Lagebild auch andere Anomalien in der analogen Welt abbilden können.**

Neben der geeigneten Sensorik und Effektorik sowie einer performanten digitalen Infrastruktur ist eine effektive Drohnenabwehr darauf angewiesen, dass die **Sensordaten heterogener Sensorlandschaften zu einem umfassenden Drohnen-Lagebild aggregiert** werden und dieses Lagebild auch den zuständigen Sicherheitsbehörden sowie betroffenen Betreibern für eine schnelle sowie informierte Entscheidung über den Einsatz von Effektorik oder anderen Maßnahmen (etwa angepasste Netzführung) vorliegt.

Die Industrie könnte auf der Grundlage bestehender und erprobter Lösungen **spezifische Schnittstellen ausprägen und eine KI-gestützte Lösung für die Data-Fusion** bereitstellen, die auch die Integration von unterschiedlichen Sensoriken ziviler Betreiber erlaubt.

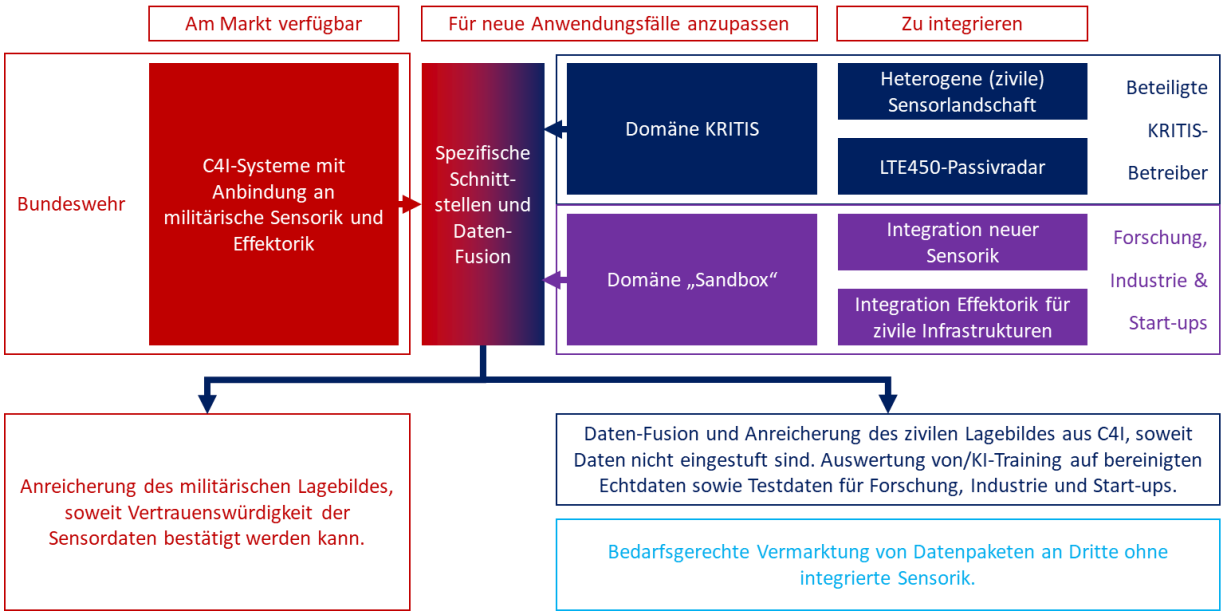

Abbildung 1: *Mögliche Architektur für gemeinsame Schnittstellen zur Integration heterogener Sensorlandschaften und Anbindung ziviler, behördlicher und militärischer Nutzer.*

Umgekehrt könnten militärische C4I-Systeme (Command, Control, Communications, Computers, and Intelligence) so auf die Daten ziviler Sensorlandschaften zurückgreifen können. Hierdurch könnte das militärische Lagebild etwa angereichert werden durch die Nahbereichsdaten von Sensoriken wie dem LTE450-Passivradar, das gegenwärtig vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE und dem BDEW entwickelt wird und das hochverfügbare 450-MHz-Funknetz als Beleuchterinfrastruktur zur Drohnendetektion nutzt (siehe Abbildung 1).

Der Vorteil einer Ausprägung spezifischer Schnittstellen auf der **Grundlage marktverfügbarer C4I-Systeme** besteht dabei in der **Verfügbarkeit erprobter und schon im Einsatz befindlicher Lösungen.** Schließlich ließe sich durch verschiedene Einsatzdomänen für Bundeswehr, Sicherheitsbehörden, Betreiber, Industrie, Start-ups und Forschung **ein Ökosystem zur agilen Weiterentwicklung von Sensorik und Effektorik** und dem **Training der KI-gestützten Sensor-Fusion-Lösung** aufbauen. **Hierdurch könnten Innovationszyklen verkürzt und Kosten gesenkt werden.**

Ansprechpartner

Mathias Böswetter
Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik
+49 30 300 199-1526
mathias.boeswetter@bdew.de