HDKZ Policy Paper Series, Nr. 1 (August 2026)

Drohnenbedrohungen: Von Einzelmaßnahmen zu einer wirksamen Schutzarchitektur

Der Drohnenvorfall am Flughafen Leipzig/Halle hat eine intensive Debatte über die Drohnenabwehr in Deutschland ausgelöst. Die politischen Antworten konzentrieren sich bislang vor allem auf den Ausbau staatlicher Abwehrkapazitäten: mehr Personal, mehr Abwehrtechnik und zusätzliche Standorte. Diese Maßnahmen sind notwendig. Sie lösen jedoch das grundlegende Problem beim Schutz Kritischer Infrastrukturen nicht.

Die entscheidende Frage reicht über den Ausbau staatlicher Abwehrkapazitäten hinaus und setzt früher an: Wie kann unter den Bedingungen einer wachsenden und sich technologisch schnell verändernden Drohnenbedrohung ein wirksamer und zugleich realistischer Schutz Kritischer Infrastrukturen organisiert werden? Der Fachdialog Drohnendetektion und -abwehr des Hessischen Drohnenkompetenzzentrums (HDKZ) mit Betreibern Kritischer Infrastrukturen, Polizei, Luftfahrtakteuren und Technologieanbietern zeigt dafür vier zentrale Handlungsfelder:

Risiken bewerten und Lagekenntnis schaffen: Betreiber von KRITIS (im weiteren Sinn) müssen eine risikobasierte Kosten-Nutzen-Abwägung darüber treffen, welche Anlagen und Funktionen welchen Schutz benötigen. Dafür fehlt ihnen heute vielfach eine entscheidende Grundlage: belastbare Informationen darüber, welche Drohnenaktivitäten in ihrem Umfeld stattfinden.

Technische Lücken durch Sensorfusion schließen: Die Annahme, die notwendige Technik sei bereits vorhanden und müsse lediglich eingesetzt werden, greift zu kurz. Leistungsfähige Einzelsysteme existieren zwar, doch unterschiedliche Detektionstechnologien weisen jeweils spezifische Stärken und Grenzen bei der Erfassung verschiedener Drohnentypen und Bedrohungsszenarien auf. Auch Fehlerraten und die kontinuierliche Anpassung an neue Drohnentechnologien bleiben Herausforderungen.

Reaktionsfähigkeit statt Zuständigkeitsdebatte: Das in der öffentlichen und politischen Debatte immer wieder angeführte „Kompetenzwirrwarr“ trifft den Kern des Problems nicht. Die Zuständigkeiten sind eindeutig geregelt. Die Schwachstelle liegt vielmehr darin, dass Abstimmungs-, Entscheidungs- und Freigabeprozesse länger dauern können als das verfügbare Interventionsfenster von meist nur 2-3 Minuten.

Schutz und Resilienz differenzieren: Nicht jede Kritische Infrastruktur kann flächendeckend gegen Drohnen geschützt werden. Insbesondere bei weit verzweigten leitungsgebundenen Infrastrukturen stößt ein objektbezogener Schutz technisch und wirtschaftlich an Grenzen.

Die Konsequenz daraus ist ein Perspektivwechsel: Nicht der Ausbau einzelner Abwehrkomponenten, sondern die Herstellung einer durchgängigen Schutz- und Reaktionsfähigkeit muss im Mittelpunkt der Diskussion stehen. Dafür sind vier Maßnahmen prioritär:

1. Lagekenntnis im unteren Luftraum schaffen

Grundlage eines belastbaren Lagebildes ist die eindeutige Identifizierbarkeit des regulären Drohnenverkehrs. Die Registrierungspflicht sollte deshalb künftig am Fähigkeitsprofil des Luftfahrzeugs ansetzen und jedes Gerät erfassen, das über eine automatische Flugführung, einen nicht sichtverbindungsgebundenen Datenlink oder eine Nutzlastschnittstelle verfügt – unabhängig davon, ob es serienmäßig oder individuell gefertigt wurde. Die bestehende Regelung für den klassischen Modellflug bleibt davon unberührt. Genehmigte Modellfluggelände sollten zugleich als bekannte Betriebsräume in die Lagebilder einfließen.

Die Registrierung wird potenzielle Angreifer zwar nicht identifizieren, ermöglicht aber, den kooperativen Drohnenverkehr möglichst vollständig abzubilden. Erst vor diesem Hintergrund wird ein nicht identifizierbares Flugobjekt zu einem belastbaren Anhaltspunkt für eine abgestufte Reaktion. Bestehende und künftig verfügbare Möglichkeiten der Fernidentifizierung müssen deshalb so weiterentwickelt und verfügbar gemacht werden, dass berechtigte Stellen und Betreiber Kritischer Infrastrukturen kooperative Drohnen automatisiert erkennen und von nicht identifizierbaren Flugobjekten unterscheiden können.

Darauf aufbauend ist eine gestufte Lagebildarchitektur erforderlich, in der Informationen auf unterschiedlichen Aggregationsebenen bedarfsgerecht zusammengeführt und den jeweils berechtigten Akteuren zugänglich gemacht werden. Neue Modelle für die Bereitstellung solcher Lageinformationen sollten dabei berücksichtigt werden.

2. Sensorfusion systematisch weiterentwickeln und erproben

Für eine verlässliche Drohnendetektion reicht kein einzelnes Sensorprinzip aus. Multi-Sensor-Systeme sind bereits verfügbar; ihre Leistungsfähigkeit hängt jedoch wesentlich von Einsatzumgebung, Bedrohungsszenario und der Qualität der Sensorfusion ab. Unterschiedliche Verfahren (u. a. RF-Sensorik, Radar, EO/IR, akustische Sensorik und LiDAR) besitzen jeweils spezifische Stärken und Grenzen.

Bund und Länder sollten deshalb die Weiterentwicklung und kontinuierliche Erprobung von Multi-Sensor-Systemen gezielt fördern. Im Mittelpunkt müssen die zuverlässige Detektion und Klassifizierung, geringe Fehlerraten, die Qualität der Sensorfusion sowie die kontinuierliche Anpassung an neue Drohnentechnologien und Bedrohungsszenarien stehen.

3. Reaktionszeiten verkürzen – Betreiberbefugnisse risikobasiert ermöglichen

Interventionsfenster von teilweise nur zwei bis drei Minuten lassen im Akutfall keinen Raum für mehrstufige Abstimmungs- und Freigabeprozesse. Besser abgestimmte Kommunikation allein löst dieses strukturelle Zeitproblem nicht –

die Reaktionskette selbst muss verkürzt werden.

Wo eine rechtzeitige staatliche Intervention nicht gewährleistet werden kann, sollten die Länder prüfen, qualifizierten Betreibern besonders schutzbedürftiger Kritischer Infrastrukturen klar begrenzte Befugnisse zur Detektion und Intervention zu übertragen. Das bereits in einem Bundesland geplante Modell einer freiwilligen, zeitlich und sachlich begrenzten Beleihung weist hierfür einen möglichen Weg. Die hoheitliche Gesamtverantwortung verbleibt beim Staat.

4. Schutz und Resilienz risikobasiert verbinden

Betreiber Kritischer Infrastrukturen müssen Drohnenbedrohungen systematisch in ihre Risiko- und Resilienzplanung einbeziehen. Dazu gehört, kritische Anlagen und Funktionen zu identifizieren, mögliche Angriffsszenarien und deren Auswirkungen zu bewerten sowie festzulegen, wo Detektion und Schutz erforderlich und verhältnismäßig sind. Für Bereiche, in denen ein wirksamer Schutz nicht gewährleistet werden kann, ist Vorsorge für den Schadensfall zu treffen, etwa durch Redundanzen, vorbereitete alternative Betriebsweisen, Business Continuity und Konzepte zur schnellen Wiederherstellung der Funktionsfähigkeit.

Technologische Souveränität als Querschnittsanforderung

Der Aufbau einer wirksamen Schutzarchitektur muss zugleich die technologische Souveränität Deutschlands und Europas stärken. Dies betrifft die gesamte Fähigkeitskette – von Sensorik und Sensorfusion über Datenverarbeitung und Lagebilder bis zu Abwehrsystemen. Bei sicherheitskritischen Technologien müssen strategische Abhängigkeiten von Nicht-EU-Drittstaaten reduziert und die Kontrolle über kritische Komponenten, Daten und Systemfunktionen gewährleistet werden. Europäische und deutsche Fähigkeiten sind deshalb gezielt zu stärken.

Fazit

Deutschland braucht neben Abwehrtechnik und staatlichen Einsatzkräften eine risikobasierte Schutz- und Resilienzstrategie, die Transparenz im unteren Luftraum schafft, technologische Fähigkeitslücken schließt, Reaktionsketten an die Geschwindigkeit der Bedrohung anpasst und dort, wo Schutz an seine Grenzen stößt, die schnelle Wiederherstellung der Funktionsfähigkeit.

Kontakt
Prof. Dr. Michèle Knodt
Direktorin Hessisches
Drohnenkompetenzzentrum
06151 16 57353
knodt@pg.tu-darmstadt.de

Prof. Dr. Uwe Klingauf
Direktor Hessisches
Drohnenkompetenzzentrum
06151 16 21040
klingauf@fsr.tu-darmstadt.de

Kofinanziert von der Europäischen Union
HESSEN Hessisches Ministerium für Digitalisierung und Innovation
TECHNISCHE UNIVERSITÄT DARMSTADT