

BESCHLUSS

des Bundesvorstands der FDP, Berlin, 13. September 2026

KRITIS schützen – Deutschland resilient gegen hybride Bedrohungen machen

Der Bundesvorstand der Freien Demokraten stellt fest, dass Deutschland Ziel hybrider Kriegsführung ist. Der Fund einer mit einer Sprengvorrichtung versehenen Drohne am Flughafen Leipzig/Halle im August 2026 und die Heraufstufung der Gefährdungslage durch das Bundesinnenministerium markieren eine neue Qualität. Der Gesetzgeber hat mit dem KRITIS-Dachgesetz und dem Zweiten Gesetz zur Änderung des Luftsicherheitsgesetzes im März 2026 erste Rahmen geschaffen. Beide bleiben in der Anwendung lückenhaft, weil Zuständigkeiten unklar, Reaktionsketten unverbindlich und Befugnisse und Fähigkeiten voneinander getrennt sind. Zudem darf Deutschland sich nicht auf die passive Abwehr einzelner Angriffe beschränken. Erforderlich ist eine Strategie, die auch gegnerische Strukturen und Handlungsmöglichkeiten frühzeitig identifiziert, gezielt beeinträchtigt und die staatliche Initiative wiederherstellt.

Der Bundesvorstand fordert daher:

I. Lagebild und strategische Aufklärung

1. Für Betreiber kritischer Anlagen und Organisationen des Bevölkerungsschutzes sind rechtssichere und verlässliche Informations- und Kommunikationswege zu den zuständigen Sicherheitsbehörden zu gewährleisten. Sicherheitsrelevante Erkenntnisse müssen schnell an betroffene Betreiber gelangen; umgekehrt müssen Betreiber relevante Beobachtungen unkompliziert an die zuständigen Stellen übermitteln können. Die Vertraulichkeit nachrichtendienstlicher Erkenntnisse und der geschützte Informationsaustausch innerhalb der gemeinsamen Zentren bleiben dabei gewährleistet.
2. Für das Gemeinsame Zentrum zur Abwehr hybrider Bedrohungen und das Gemeinsame Drohnenabwehrzentrum ist eine eigene gesetzliche Grundlage zu schaffen. Sie regelt Aufgaben, Beteiligte, Datenverarbeitung, Zweckbindung und Löschfristen. Die parlamentarische Kontrolle der Zentren und der in ihnen mitwirkenden Behörden muss im Rahmen der jeweils bestehenden parlamentarischen Kontrollzuständigkeiten jederzeit gewährleistet bleiben. Am Trennungsprinzip zwischen Polizei und Nachrichtendiensten wird festgehalten. Die Zentren bleiben Koordinierungsplattformen und werden keine eigenständigen Behörden mit Weisungsbefugnis.
3. Weitere Abwehrzentren werden nicht gegründet. Bestehende Strukturen sind zu konsolidieren. Die Bundesregierung legt dem Bundestag eine Übersicht

über Aufgaben, Schnittstellen und Doppelstrukturen der bestehenden Zentren vor.

4. Wer Informationen freiwillig mit den Sicherheitsbehörden teilt, darf dadurch nicht in Haftung oder Bußgeldverfahren geraten. Freiwillig geteilte Erkenntnisse dürfen nicht als Grundlage aufsichtsrechtlicher Sanktionen gegen den mitteilenden Betreiber verwendet werden.

II. Gesamtstaatliche Architektur und Reaktionsketten

1. Der vom Nationalen Sicherheitsrat beschlossene Aktionsplan zur Abwehr hybrider Bedrohungen ist in ein verbindliches und überprüfbares Gesamtkonzept zu überführen. Dieses ordnet je Infrastrukturtyp zu, wer erkennt, wer bewertet, wer entscheidet und wer wirkt. Es enthält verbindliche Alarmierungs- und Reaktionszeiten, die vorab festgelegt und nicht im Ereignisfall improvisiert werden.
2. Die nach dem KRITIS-Dachgesetz von den Ländern benannten zentralen Ansprechpartner sind zu leistungsfähigen Schnittstellen für die Lagebewältigung auszubauen. Sie müssen durchgehend erreichbar sein, über definierte Reaktionszeiten verfügen und an das Gemeinsame Drohnenabwehrzentrum sowie das Gemeinsame Zentrum zur Abwehr hybrider Bedrohungen angebunden sein. Ihre bisherige Funktion als zentraler Ansprechpartner für die Durchführung des KRITIS-Dachgesetzes reicht für die operative Bewältigung hybrider Lagen nicht aus.
3. Die bereits vorgesehene gemeinsame Meldestelle von Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie Bundesamt für Sicherheit in der Informationstechnik (BSI) ist zu einem echten Once-Only-Verfahren auszubauen. Betreiber sollen einen Vorfall nur einmal melden müssen. Diese Meldung muss, soweit unionsrechtlich zulässig, zugleich sämtliche parallelen bundesrechtlichen Meldepflichten erfüllen. Mehrfachmeldungen desselben Sachverhalts an unterschiedliche staatliche Stellen sind zu vermeiden.
4. Bund und Länder üben gestuft. Sektorale Übungen finden jährlich statt, gesamtstaatliche Übungen mindestens alle zwei Jahre nach dem Vorbild skandinavischer Gesamtverteidigungsübungen. Die Auswertung wird in einer nicht eingestuften Fassung veröffentlicht und enthält verbindliche Umsetzungsfristen für die festgestellten Mängel.
5. Auf eine gesetzliche Legaldefinition des Begriffs hybride Bedrohung, an die Meldepflichten anknüpfen, wird verzichtet. Melde- und Registrierungspflichten bleiben ursachenneutral, weil die Zurechnung zu einem fremden Staat Monate dauern kann, eine Meldung aber innerhalb von Stunden erfolgen muss. Stattdessen wird der Begriff der hybriden Lage allein als Eskalationsstufe im Koordinierungs- und Gefahrenabwehrrecht definiert. Anknüpfungspunkt sind tatsächliche Anhaltspunkte für ein koordiniertes, fremdstaatlich veranlassetes Vorgehen, in Anlehnung an die Formulierung des neuen Paragraphen 15a des Luftsicherheitsgesetzes.
6. Die zwischen den fünf norddeutschen Küstenländern vereinbarte Zusammenarbeit bei Detektion und Abwehr einschließlich abgestimmter Beschaffung ist Vorbild für eine bundesweite Beschaffungs Kooperation. Sechzehn getrennte Beschaffungsverfahren für dieselbe Technik sind teuer und erschweren die ge-

meinsame Lagebewältigung. Die Zusammenarbeit ist an das Europäische Kompetenzzentrum für die Abwehr hybrider Bedrohungen in Helsinki sowie an die NATO-Initiativen zum Schutz von Seekabeln in der Ostsee anzubinden.

III. Vom Erkennen zum Wirken - gestufte Abwehrbefugnisse in der Drohnenabwehr

1. Die Novelle des Bundespolizeigesetzes ist nach der erforderlichen Wiederholung der Schlussabstimmung zügig zu verabschieden, soweit sie Detektions- und Abwehrbefugnisse gegen unbemannte Luftfahrzeuge betrifft. Die im selben Gesetz vorgesehene automatisierte biometrische Echtzeiterkennung im öffentlichen Raum ist herauszulösen und abzulehnen. Drohnenabwehr rechtfertigt keine flächendeckende Gesichtserkennung.
2. Die Bundespolizei und jede Landespolizei brauchen eigene, einsatzfähige Einheiten und Technik zur Drohnendetektion und Drohnenabwehr. Der neue Paragraph 15a des Luftsicherheitsgesetzes, der eine Befugnis der Streitkräfte zur Abwehr unbemannter Luftfahrzeuge vorsieht, schließt die Abwehrlücke nur für besonders schwere Unglücksfälle. Für die alltägliche Lage nicht kooperativer Drohnen über Häfen, Umspannanlagen, Rechenzentren und Verkehrswegen bleibt sie offen.
3. Betreibern kritischer Anlagen ist der rechtssichere Einsatz der für den Schutz ihrer Anlagen erforderlichen technischen Mittel zur Drohnendetektion zu ermöglichen. Dabei ist ein technologieoffener Einsatz passiver und aktiver Detektionssysteme zu ermöglichen. Die Maßnahmen müssen auf den Schutz der jeweiligen kritischen Anlage ausgerichtet und verhältnismäßig sein und dürfen keine allgemeine Überwachungsbefugnis begründen.
4. Eine Übertragung robuster Abwehrbefugnisse auf Betreiber im Wege der Beileihung ist bundeseinheitlich zu regeln. Die übertragenen Befugnisse und zulässigen Wirkmittel sind gesetzlich abschließend zu bestimmen und auf die Abwehr konkreter Gefahren für die jeweils geschützte kritische Anlage zu begrenzen. Eine allgemeine Übertragung polizeilicher Gefahrenabwehrbefugnisse auf private Betreiber ist ausgeschlossen. Der Einsatz von Wirkmitteln erfolgt nach einem gesetzlich festgelegten Eskalationsprinzip und unterliegt besonderen Anforderungen an Zielidentifikation, räumliche Begrenzung, Risikominimierung, Dokumentation und technische Fail-Safe-Mechanismen.
5. Maßgeblich für Abwehrmaßnahmen ist die von einem unbemannten Luftfahrzeug konkret ausgehende Gefahr, nicht die Eigentumslage am überflogenen Grundstück. Bei der Gefahrenbewertung sind insbesondere elektronische Identifizierbarkeit und Registrierung, Flugverhalten, das Eindringen in geschützte Bereiche, die Reaktion auf Anweisungen und sonstige konkrete Gefahrenindikatoren zu berücksichtigen. Ordnungsgemäß betriebene gewerbliche und behördliche Drohnennutzung darf nicht unter Generalverdacht geraten. Voraussetzung ist der zügige Aufbau der elektronischen Fernidentifizierung und der Luftraumdienste für unbemannte Luftfahrt. Gewerbliche, private und behördliche Drohnennutzung darf nicht unter Generalverdacht geraten.
6. Wirkmittel sind gestuft einzusetzen, von der Übernahme der Steuerung über nicht kinetische Verfahren bis zum physischen Abfangen. Kinetische Wirkung über bewohntem Gebiet bleibt hoheitlichen Kräften vorbehalten. Das Risiko herabfallender Teile ist bei der Verhältnismäßigkeitsprüfung ausdrücklich zu berücksichtigen.

IV. Resilienz von Anfang an mitplanen

1. Resilienz Anforderungen sind stärker bereits in Planungs- und Genehmigungsverfahren zu berücksichtigen. Die Betreiberpflichten des KRITIS-Dachgesetzes gewährleisten bislang keine hinreichende frühzeitige Integration von Resilienz Anforderungen in das einschlägige Planungs- und Genehmigungsrecht. Insbesondere bei Offshore-Windenergie, Netzanbindungen und Seekabeln müssen verhältnismäßige Detektions- und Schutzanforderungen deshalb bereits bei Planung und Genehmigung berücksichtigt werden.
2. Für maritime Infrastrukturen ist die im Dachgesetz begonnene Systematik auszubauen. Der Begriff der maritimen Infrastrukturen, die Berücksichtigung ihrer Besonderheiten in den nationalen Risikoanalysen und die Zusammenarbeit von Bundesamt für Seeschifffahrt und Hydrographie und Bundesnetzagentur in der ausschließlichen Wirtschaftszone sind gesetzlich angelegt, aber nicht mit Fähigkeiten und Zuständigkeiten für die Abwehr unterlegt.
3. Die Rechtsverordnung zu kritischen Dienstleistungen und Schwellenwerten ist zu nutzen, um die tatsächliche Kritikalität einer Anlage stärker abzubilden. Neben der Zahl versorgter Einwohner sind. Insbesondere regionale Monopolstellungen, fehlende Substituierbarkeit, Abhängigkeiten anderer kritischer Dienstleistungen und mögliche Kaskadeneffekte zu berücksichtigen. Eine pauschale Ausweitung regulatorischer Pflichten allein durch niedrigere Schwellenwerte ist zu vermeiden.
4. Kommunale Betreiber und kommunale Aufgabenträger sind einzubeziehen. Stadtwerke, Hafenbetriebe und kommunale Wasserversorger tragen wesentliche Teile der Versorgung, fallen aber häufig unter die Schwellenwerte. Bund und Länder stellen die für die Umsetzung erforderlichen Mittel bereit.

V. Cyber-physische Resilienz

1. Die Risikoanalysen nach dem KRITIS-Dachgesetz und das Risikomanagement nach dem BSI-Gesetz sind systematisch zu verzahnen. Physische und cyberbezogene Risikoanalysen sollen auf einer gemeinsamen Betrachtung von Risiken, Abhängigkeiten und Kaskadeneffekten aufbauen. Bereits erhobene Informationen und erbrachte Nachweise sind nach dem Once-Only-Prinzip wiederzuverwenden. Doppelte Erhebungs-, Dokumentations- und Nachweispflichten sind zu vermeiden.
2. Für die Sicherheit von Betriebstechnik sind eigene Mindeststandards neben denen der klassischen Informationstechnik zu entwickeln. Steuerungssysteme lassen sich nicht nach den Regeln der Büro-Informationstechnik absichern. Der Staat darf dabei nicht selbst zur Sicherheitslücke werden, wie jüngst in Berlin geschehen. Wer sensible Infrastrukturinformationen von Betreibern verlangt, muss sie wirksam schützen. Behörden sollen nur die Daten anfordern und vorhalten, die sie tatsächlich benötigen. Gelangen Schutzkonzepte oder Zugangsinformationen in fremde Hände, müssen betroffene Betreiber unverzüglich gewarnt und Schutzmaßnahmen angepasst werden.
3. Das Bundesamt für Sicherheit in der Informationstechnik ist personell auszubauen und gleichzeitig aus der Aufsicht des Bundesinnenministeriums zu lösen und als unabhängige Behörde zu führen. Kapazität ohne Unabhängigkeit löst den Interessenkonflikt zwischen Schließen und Offenhalten von Sicherheitslücken nicht.

4. Kleine und mittlere Unternehmen brauchen Beratung statt zusätzlicher Berichtspflichten. Vorlagen, Muster und Branchenstandards sind vorrangig vor Einzelfallaufgaben. Pflichten müssen sich an Kritikalität, Risiko und Leistungsfähigkeit des Betreibers orientieren. Insbesondere kleinere Betreiber, die allein aufgrund ihrer regionalen Systemrelevanz erfasst werden, dürfen nicht automatisch denselben administrativen Anforderungen unterliegen wie große überregionale Betreiber.
5. Für sicherheitskritische Informations- und Betriebstechnik sowie Sensorik ist eine verbindliche, risikobasierte Vertrauenswürdigkeits- und Lieferkettenprüfung vorzusehen. Anbieter und Komponenten sind auszuschließen, wenn aufgrund staatlicher Einfluss- oder Kontrollmöglichkeiten, rechtlicher Zugriffsverpflichtungen gegenüber Drittstaaten, ihrer Eigentümer- und Governance-Struktur oder sonstiger konkreter Umstände ein nicht hinnehmbares Sicherheitsrisiko besteht.

VI. Finanzierung

1. Neue Sondervermögen werden abgelehnt. Die Schuldenbremse bleibt unangestastet.
2. Investitionen in die Härtung kritischer Infrastruktur sind auf die im Haager Verteidigungsinvestitionsplan vorgesehene Komponente von bis zu 1,5 Prozent des Bruttoinlandsprodukts für verteidigungs- und sicherheitsrelevante Ausgaben anzurechnen. Der Schutz kritischer Infrastruktur, die Verteidigung der Netze und die Zivilvorsorge sind dort ausdrücklich genannt. Sicherheit in Zeiten hybrider Bedrohung ist nicht auf Streitkräfte beschränkt, sie erfordert aber keinen neuen Schuldentopf, sondern eine ehrliche Zuordnung und Priorisierung innerhalb der bestehenden Verpflichtung.
3. Werden Betreibern hoheitliche Aufgaben übertragen oder Schutzpflichten auferlegt, ist die Kostentragung mitzuregeln. Eine vollständige Kostenlast bei den Betreibern ohne staatliche Beteiligung führt dazu, dass gerade kleinere und kommunale Betreiber ungeschützt bleiben.
4. Übertragen Bund oder Länder den Kommunen neue Aufgaben im Bereich der Resilienz, ist die Finanzierung gleichzeitig zu regeln.