P o s i t i o n s p a p i e r

Hybride Angriffe entschlossen abwehren
Staatliche Resilienz stärken
Kritische Infrastruktur schützen

Beschluss
vom 7. März 2026

A n s p r e c h p a r t n e r d e r K o n f e r e n z

Vorsitzender **Dr. Christos Katzidis, Nordrhein-Westfalen**
Platz des Landtags 1, 40221 Düsseldorf, Tel: 0211 8842186, christos.katzidis@landtag.nrw.de

Stv. Vorsitzende **Marco Lübke MdBB, Bremen**
Am Wall 135, 28195 Bremen, Tel: 0421 308940, luebke@cdu-bremen.de

Ann Christin von Allwörden MdL, Mecklenburg-Vorpommern
Lennéstraße 1, 19053 Schwerin, Tel: 0385 5252215, vonallwoerden@cdu.landtag-mv.de

Seit dem russischen Angriffskrieg gegen die Ukraine hat sich die sicherheitspolitische Lage in Europa grundlegend verändert. Krieg ist nach Jahrzehnten relativer Stabilität nach Europa zurückgekehrt und mit ihm eine neue Qualität hybrider Bedrohungen. Sabotageakte, Cyberangriffe, Desinformationskampagnen, Drohnenspionage und sog. Spezialoperationen sind längst Teil einer strategischen Auseinandersetzung autoritärer Staaten mit den freiheitlichen Demokratien Europas.

Aggressive Akteure wie Russland setzen hybride Mittel systematisch ein, um westliche Gesellschaften zu destabilisieren, Vertrauen in staatliche Institutionen zu untergraben und kritische Infrastruktur anzugreifen. Hinzu kommen nichtstaatliche Akteure: extremistische Gruppierungen, transnationale kriminelle Netzwerke, radikalisierte Einzeltäter sowie hochprofessionelle Hacker- und Cybergruppierungen, die zunehmend grenzüberschreitend und arbeitsteilig agieren.

Hybride Bedrohungen operieren bewusst unterhalb der Schwelle eines offenen militärischen Konflikts. Ihr Ziel ist es, Gesellschaften zu verunsichern, staatliche Strukturen zu überlasten und strategische Verwundbarkeiten auszunutzen. Besonders gefährdet ist unsere kritische Infrastruktur – Energieversorgung, Kommunikationsnetze, Wasserversorgung, Verkehrssysteme und digitale Steuerungsstrukturen. Die Anschläge auf Pipelines, Cyberangriffe auf Behörden und Unternehmen sowie zunehmende Spionageeinsätze von Drohnen über sensiblen Einrichtungen zeigen, dass Deutschland längst im Fokus hybrider Angriffe, Einfluss- und Störmaßnahmen steht.

Diese Entwicklungen sind Ausdruck einer verschärften weltpolitischen Lage, in der systemische Rivalität und geopolitische Machtkonflikte zunehmen. Deutschland darf diesen Herausforderungen nicht defensiv oder reaktiv begegnen. Es braucht eine umfassende Strategie zur Stärkung staatlicher Resilienz, klar definierte Zuständigkeiten, moderne Schutzmechanismen und eine robuste Sicherheits-architektur, die auch unter extremen Belastungen handlungsfähig bleibt.

Die innenpolitischen Sprecherinnen und Sprecher der Union setzen sich deshalb für einen konsequenten Maßnahmenkatalog ein, der Schutz, Prävention, Abschreckung und schnelle Reaktionsfähigkeit verbindet. Ziel ist es, Deutschlands Souveränität zu sichern, die Resilienz der Bevölkerung zu stärken, sie zu schützen und unsere kritischen Infrastrukturen widerstandsfähig gegen hybride Angriffe zu machen.

Wir sind der Überzeugung, dass Deutschland mit dem nachfolgenden 10-Punkte-Plan im Bereich der Sicherheitsarchitektur, Drohnenabwehr und Krisenkommunikation über Notstrom- und Trinkwasserversorgung bis hin zu Cybersicherheit, Schutzräumen und einer strukturellen Stärkung von Bundeswehr und Katastrophenschutz besser aufgestellt sein wird.

10-Punkte-Plan für mehr Schutz, Ordnung und Souveränität

1. Schutz Kritischer Infrastruktur durch den Einsatz von Drohnen und anderer geeigneter Abwehrmaßnahmen

Unbemannte Luftsysteme werden zunehmend für Aufklärungszwecke und Angriffe auf sicherheitsrelevante Einrichtungen eingesetzt. Gleichzeitig dienen Drohnen auch dem Schutz von KRITIS-Anlagen und bieten erhebliche Vorteile bei der Luftraumüberwachung und der Lagebilderstellung. Mit der Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) hat das Land Berlin bereits eine klare gesetzliche Grundlage für den Einsatz und die Abwehr von unbemannten Luftsystemen geschaffen, so wie andere Bundesländer auch (Bayern, Bremen, Rheinland-Pfalz, Hessen). Wir fordern die übrigen Länder auf, vergleichbare Befugnisse in ihren Polizeigesetzen zu verankern, um den rechtssicheren Einsatz zur Gefahrenabwehr unter klar definierten Voraussetzungen zu gewährleisten. Dies gilt im gleichen Maße für den Einsatz von Videobeobachtung und KI im öffentlichen Raum. Dabei müssen gezielt finanzielle Mittel für den Aufbau von Drohneneinheiten, moderner Sensorik, Radaranlagen sowie Abwehrtechnik bereitgestellt werden. Die Kooperation der Landespolizeien mit der Bundespolizei und der Bundeswehr sowie weiterer Verantwortlichen und Behörden ist weiter auszubauen und strukturell zu verankern. In diesem Zusammenhang begrüßen wir die Novellierung des Luftsicherheitsgesetzes und die neu geschaffene Befugnis für die Bundeswehr, die Länder im Falle eines schweren Unglücksfalls bei der Abwehr von unbemannten Luftfahrzeugen auch mit Waffengewalt zu unterstützen. Dahingehend fordern wir die Bundesregierung auf, gemeinsam mit den Ländern und den Betreibern kritischer Infrastrukturen ein dauerhaftes, interoperables[1] und rund um die Uhr verfügbares einheitliches Lagebild in Echtzeit für unbemannte Luftfahrzeuge im unteren Luftraum zu schaffen.

2. Resilienz der Kommunikationsinfrastruktur

Die Anzahl satellitengestützter Telefone bei den Sicherheits- und Einsatzkräften ist derzeit stark begrenzt und der Digitalfunk erweist sich im Krisenfall nur bedingt zuverlässig. Diese Defizite gefährden die Führungs- und Handlungsfähigkeit im Katastrophenfall. Wir fordern den systematischen Ausbau satellitengestützter Kommunikationsmittel. Zudem bedarf es einer leistungsfähigen Sireneninfrastruktur sowie deren vollständige Integration in bestehende digitale Warnsysteme wie das Modulare Warnsystem des Bundes (MoWaS) und die Warn-App NINA. Sirenen stellen als netzunabhängiges Warnmittel eine unverzichtbare Redundanz im Falle von Cyberangriffen oder Stromausfällen dar und sind daher flächendeckend zu ertüchtigen. Der flächendeckende Wiederaufbau einer modernen, digital steuerbaren Sireneninfrastruktur muss bundesweit verbindlich vorangetrieben und durch dauerhafte Wartungs- und Investitionsprogramme abgesichert werden. Insbesondere

[1] Interoperabilität bezeichnet die Fähigkeit verschiedener Systeme, Anwendungen oder Komponenten, Informationen auszutauschen, diese Daten korrekt zu interpretieren und gemeinsam zu nutzen.

im ländlichen Raum ist der flächendeckende Ausbau digital steuerbarer Sirenen als niedrigschwellige und ausfallsichere Warnmittel prioritär umzusetzen. Der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) muss kontinuierlich modernisiert und technisch auf den neuesten Stand gebracht werden. Insbesondere müssen auch kommunale Vollzugskräfte eingebunden werden in den BOS-Funk. Das Ziel ist ein einheitliches und redundantes Krisenkommunikationsnetzwerk. Dazu zählt auch die Beschaffung von autark betriebenen und preisgünstigen Kommunikationsmitteln, die im Krisenfall den Kontakt und den Austausch mit der Bevölkerung sowie zwischen den Sicherheitsbehörden aufrechterhalten und ein Notfall-WLAN bereitstellen.
Eine verlässliche Mobilfunkversorgung ist im Krisen- und Katastrophenfall von zentraler Bedeutung für die Aufrechterhaltung staatlicher und gesellschaftlicher Handlungsfähigkeit. Umso problematischer ist es, dass Mobilfunkstandorte nicht verpflichtend mit einer Notstromversorgung ausgestattet werden müssen. Gerade bei hybriden Bedrohungslagen ist eine funktionierende Kommunikation unverzichtbar. Es muss verhindert werden, dass binnen kürzester Zeit große Teile der Mobilfunkkommunikation vollständig zusammenbrechen. Durch die Umsetzung der NIS-2-Richtlinie wurden die Anforderungen an die Sicherheit und Resilienz von Telekommunikationsnetzen im Telekommunikationsgesetz (TKG) bereits deutlich verschärft. Betreiber kritischer Telekommunikationsinfrastruktur sind verpflichtet, Maßnahmen zur Aufrechterhaltung des Betriebs und zum Krisenmanagement, auch bei länger andauernden Stromausfällen, vorzuhalten. Entscheidend ist daher eine konsequente Umsetzung dieser Vorgaben sowie eine wirksame Kontrolle durch die Bundesnetzagentur (BNetzA), damit die Mobilfunkversorgung auch in länger andauernden Gefahrenlagen zuverlässig gewährleistet bleibt.
Der öffentlich-rechtliche Rundfunk dient in einer Krisen- und Katastrophenlage als zentrale Informationsquelle für die Bevölkerung und muss jederzeit erreichbar sein. Die jeweiligen lokalen Sendestandorte und Übertragungsnetzwerke sind mit ausreichend Netzersatzanlagen für eine autarke Notstromversorgung über mehrere Tage hinweg auszustatten.

3. Notstromversorgung ausbauen

Die Erfahrungen aus vergangenen Katastrophenfällen haben aufgezeigt, dass Notstromaggregate und Netzersatzanlagen entscheidend zur Aufrechterhaltung der Versorgungslage sind. Wir fordern die Beschaffung und Vorhaltung eines ausreichend großen Bestandes in einem zentralen Treibstofflogistikkonzept, um kritische Einrichtungen im Katastrophenfall zuverlässig bedienen zu können. Auf Bundesebene sollte eine Reserve-Kapazität von Notstromaggregaten und Netzersatzanlagen vorgehalten werden, welche durch die Feuerwehr, das THW und die Bundeswehr gemeinschaftlich genutzt und ein schneller und unbürokratischer Zugang gewährleistet ist.[2] Die lokale Notstromversorgung von überlebenswichtigen

[2] Das BBK plant den Aufbau einer Notstromreserve. Bis 2029 sollen hierfür 50 Millionen Euro bereitgestellt werden (Stromausfall in Deutschland: Bundesländer-Notfallpläne im Check). Die Mitgliedsstadtwerke des Verbands kommunaler Unternehmen (VKU) fordern eine „Nationale Reserve Blackout“ (Stromausfälle: Stadtwerke fordern nationale Krisenreserve).

Einrichtungen, wie Krankenhäusern und Pflegeunterkünften, soll zudem ausgeweitet werden, insbesondere auch auf alle polizeilichen Einrichtungen des Polizeivollzugsdienstes sowie auf Tankstellen zur Sicherung der Treibstoffversorgung, die mit Notstromaggregaten auszurüsten sind.

4. Katastrophenvorsorge

Hybride Bedrohungen und Angriffe zielen darauf ab, staatliche Handlungsfähigkeit infrage zu stellen und gesellschaftliche Verunsicherung zu erzeugen. Wir fordern, dass Bund und Länder die Vermittlung grundlegender Kompetenzen zur Bewältigung von Krisensituationen deutlich ausbauen und die Eigenvorsorge nach den zentralen Empfehlungen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) unterstützen. So sollen etwa Erste-Hilfe-Kurse bereits frühzeitig im Lehrplan von Schulen verankert werden. Im Saarland gibt es seit dem Schuljahr 2025/2026 das Unterrichtsfach „Blaulicht“, das fünfstündig ab der Mittelstufe von Lehrkräften und Angehörigen aller Blaulichtorganisationen unterrichtet wird. Dieses Modell kann als Vorbild für andere Bundesländer dienen. Darüber hinaus ist die Einbindung zivilgesellschaftlicher Akteure entscheidend. Digitale Plattformen zur Koordination freiwilligen Engagements – wie das Modell der „Katastrophenschutzhelfer“[3] - sollen hierbei als Vorbild dienen, um Bürger im Krisenfall schnell und bedarfsgerecht einzubinden. Die ehrenamtlichen Helfer müssen im Krisen- und Katastrophenfall zudem unbürokratisch und schnell von ihren Arbeitgebern freigestellt werden und für ihren Einsatz angemessen entschädigt werden.
Katastrophenschutz-Leuchttürme bzw. Notfallinfopunkte sollen im Ernstfall Informationen und Hilfestellungen für die Menschen vor Ort bereithalten. Ziel ist es, dass jeder Haushalt Handlungsempfehlungen zur Vorbereitung auf einen langanhaltenden flächendeckenden Stromausfall kennt.

5. Stärkung der Einsatzbereitschaft der Bundeswehr und Kooperationen

Zum Zweck einer dauerhaft qualifizierten Personal- und Nachwuchsgewinnung fordern wir die Einführung eines verpflichtenden Gesellschaftsjahres für alle, bei dem zwischen dem militärischen Dienst und einem zivilen Dienst Wahlmöglichkeit bestehen sollte. Um die militärischen Fähigkeiten im Bereich des Heimatschutzes und die Sicherung der kritischen Infrastruktur fortlaufend garantieren zu können, fordern wir einen Aufwuchs der Heimatschutzkräfte[4] der Bundeswehr von derzeit 6.000 Soldaten auf eine Zielstruktur von mindestens 50.000 Dienstposten.[5] Zudem sollen die digitalen

[3] KatHelfer (oft spezifisch als KatHelfer-Pro) ist eine Software-as-a-Service (SaaS) Lösung von T-Systems, die Behörden und Katastrophenschutzorganisationen dabei unterstützt, spontane Helfer im Katastrophenfall digital zu koordinieren und gezielt einzusetzen. Sie dient der strukturierten Registrierung, Einteilung und Kommunikation von Helfenden.
[4] Heimatschutzkräfte sind in Deutschland speziell strukturierte Einheiten der Bundeswehr, die primär für den Schutz der Infrastruktur und die territoriale Verteidigung im Inland zuständig sind. Sie bestehen überwiegend aus Reservisten sowie freiwillig Wehrdienstleistenden (FWDL) und dienen als Bindeglied zwischen Armee und ziviler Gesellschaft.
[5] Bundeswehr (Bundeswehr stellt neue Heimatschutzdivision auf); Soldat & Technik (Aufstellungsappell der Heimatschutzdivision: künftig 6.000 Mann unter einem Kommando - S&T - Soldat & Technik).

Kapazitäten zum Schutz der militärischen Infrastruktur beim Zentrum für Cybersicherheit ausgebaut werden. Weiterhin sind bestehende Flugverbotszonen zu vergrößern und neue zu schaffen, um unerlaubte Überflüge in der Nähe von kritischen Einrichtungen frühzeitig zu verhindern. Um die allgemeine Einsatzfähigkeit zu erhöhen, sollten die Kommunikationswege bundesweit vereinheitlicht und standardisiert werden. Hierzu ist die Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundes- und den Landespolizeien, die Bundesnetzagentur (BNetzA), dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie den Betreibern von KRITIS-Anlagen auszubauen und zu intensivieren.
Zudem benötigen wir eine belastbare Datengrundlage dazu, wie viele Kräfte tatsächlich zur Verfügung stehen, da viele Angehörige der Blaulichtorganisationen in mehreren Organisationen engagiert sind und daher mehrfach gezählt werden. Erforderlich sind eine einheitliche Datenerfassung und fortlaufende Datenpflege auf Kreis- und Länderebene.

6. Zentrale Steuerung vereinheitlichen

Die dezentrale Struktur im Katastrophen- und Bevölkerungsschutz ermöglicht eine realistische Einschätzung der Lage vor Ort. Wir fordern die Einrichtung von dauerhaft tagenden Katastrophenschutz-Stäben auf Bundes- und Länderebene, die gemeinsame Lagebilder erstellen, regelmäßige Übungen durchführen und die operative Koordination übernehmen. Das Personal sollte in der Stabsarbeit erfahren und ressortübergreifend zusammengesetzt sein. Jedes Bundesland sollte zudem ein Landesamt für Bevölkerungsschutz oder eine vergleichbare zentrale Institution aufbauen, welche digitale und integrierte Leitstellen der Sicherheitsbehörden und der beteiligten Organisationen bündeln, mit einem 24/7-Lagezentrum. Zudem sollten die Zentralstellen mit Weisungsbefugnissen gegenüber den Kommunen ausgestattet sein. Weiterhin bedarf es bundesweit einheitlicher Standards für die Stabsarbeit, die bei regelmäßigen bundesweiten Schulungen und gemeinsamen Krisenübungen trainiert werden. Die Städte und Kommunen sind angehalten, ihre Einrichtungen im Bereich des Katastrophen- und Bevölkerungsschutzes auskömmlich zu finanzieren und personell vollständig zu besetzen. Um eine schnelle und bedarfsgerechte Versorgung vulnerabler Personen zu gewährleisten, sollen die Städte und Gemeinden darauf hinwirken, dass besondere Hilfebedarfe vorab angezeigt werden.

7. Material, Ausstattung & logistische Kapazitäten modernisieren und härten

Systemrelevante und kritische Einrichtungen sind einer Vielzahl von hybriden Bedrohungen ausgesetzt. Betreiber müssen sicherzustellen, dass sie mit der erforderlichen Technik und dem notwendigen Personal ausgerüstet sind, um

---

Die Heimatschutzkräfte der Bundeswehr sind zuständig für die territoriale Verteidigung der Bundesrepublik Deutschland. Zudem unterstützen sie zivile Behörden und Einrichtungen im Katastrophenfall durch logistische, personelle und medizinische Hilfeleistungen. Zu ihren Aufgaben gehört auch der Schutz kritischer Infrastruktur im Spannungs- und Verteidigungsfall und die Bewältigung von Naturkatastrophen.

ausreichend gehärtete Anlagen zu betreiben. Eine Grundlage hierfür sind Risikoanalysen und Risikobewertungen, die von den zuständigen staatlichen Stellen erarbeitet und den Betreibern zur Verfügung gestellt werden. Neuralgische Punkte innerhalb der Energieversorgung müssen zudem rund um die Uhr mit privatem Sicherheitspersonal geschützt werden. In akuten Bedrohungslagen muss auch der Einsatz der staatlichen Sicherheitsbehörden zum Schutz der kritischen Infrastruktur ermöglicht und zwingend angeordnet werden. Ein effektiver Katastrophen- und Bevölkerungsschutz erfordert über ausreichend Lagerkapazitäten für benötigte Materialien und Notfallvorräte. Wir fordern, regionale Katastrophen-schutz-Zentren zu schaffen, die als Materiallager, Werkstätten im 24/7-Betriebund zugleich als Räumlichkeiten für Umkleiden, Ausbildung und Verwaltung der Einsatzkräfte dienen. Einheitliche Verfahren und Logistikstandards sollen gewährleisten, dass alle Länder, Bezirke und Kommunen vergleichbare Fähigkeiten vorhalten. Aufbauend darauf soll ein bundesweit verfügbares Lagebild geschaffen und kontinuierlich mit tagesaktuellen Informationen zur Bestandsübersicht, auch unter Nutzung von künstlicher Intelligenz, gepflegt werden.
Ein weiterer zentraler Baustein ist die Stärkung der Wiederherstellungsfähigkeit nach Schadensereignissen. Kritische Infrastrukturen müssen nach Ausfällen möglichst schnell wieder arbeitsfähig werden. Dazu gehört, dass Unternehmen der kritischen Infrastruktur eigene Notfall- bzw. Energieversorgungseinheiten vorhalten, um zentrale Funktionen auch bei Stromausfällen oder Störungen aufrechterhalten können.

8. Nationales Schutzraumkonzept

Laut dem BBK bestehen derzeit noch bundesweit 579 öffentliche Schutzräume mit einer Gesamtkapazität von knapp 500.000 Schutzplätzen.[6] Doch funktionsfähig und für den Ernstfall gewappnet ist keiner. Die Bundesregierung arbeitet an einem nationalen Schutzraumkonzept unter Beteiligung der Bundesländer. Bereits bestehende Infrastruktur und Gebäude sollen hierbei als Schutzräume ertüchtigt und kenntlich gemacht werden. Im Not- und Krisenfall sollen die Bürger mittels digitaler Applikationen über den aktuellen Standort der Schutzeinrichtungen informiert werden. Wir fordern, das nationale Schutzraumkonzept schnell zu implementieren und geeignete Räumlichkeiten verbindlich zu identifizieren. Dabei sollte vor allem auch der Schutz vor Angriffen durch moderne Raketen und unbemannten Waffensystemen in die baulichen Planungen miteinbezogen werden. Für die Ertüchtigung von Schutzräumen muss der Bund in den kommenden Jahren finanzielle Mittel im zweistelligen Milliardenbereich bereitstellen. Zu prüfen wäre in diesem Zusammenhang auch, bei infrastrukturellen Neubauten geeignete bauliche Schutzraumkapazitäten mit in die Planungen zu integrieren, sodass diese im Krisenfall zügig zur Verfügung gestellt und nutzbar gemacht werden können. Dabei müssen auch die Städte und Kommunen Planungssicherheit haben und vorab allgemeine Standards definiert sein, wie viele und welche Materialien und Vorräte verbindlich vorgehalten werden müssen. Zudem fordern wir die Vorhaltung und Ertüchtigung von zentralen Unterbringungsplätzen für die Bevölkerung.

[6] Deutscher Bundestag (Drucksache 20/14631).

9. Cybersicherheit stärken

Ein effektiver Schutz Kritischer Infrastrukturen erfordert eine robuste Cybersicherheitsstrategie. Dazu gehört, dass alle sicherheitsrelevanten Verwaltungen, Behörden und IT-Betreiber regelmäßige, gemeinsame Übungen durchführen, bei denen Cyberangriffe simuliert und die Beschäftigten in Cyber-Abwehrmaßnahmen geschult werden. Wir fordern konkret, dass Red-Team-Übungen dauerhaft und strukturell verankert werden.[7] Weiterhin ist der Ausbau der Cyberabwehrkapazitäten der öffentlichen IT-Netzwerke konsequent voranzutreiben. Hierunter zählt auch die Ausstattung mit Netzersatzanlagen für die Kernnetze und eine institutionalisierte Kooperation mit dem BSI.

10. Gewährleistung krisenfester Trinkwassersysteme

Die Resilienz der Trinkwasserversorgung ist ein wesentlicher Faktor, um auch bei einem länger anhaltenden Katastrophenfall die Versorgung der Bevölkerung sicherstellen zu können. Wir fordern, Notstrom-Kapazitäten auch an dezentralen Standorten zu erweitern und zusätzliche Notwasserbrunnen zum Erhalt der Wasserversorgung zu errichten. Zudem bedarf es einer regelmäßigen Wartung und Härtung der Infrastruktur zur Sicherstellung der Trinkwasserversorgung.

[7] Ein Red Team ist eine - in der Regel - spezialisierte, unabhängige Gruppe von Sicherheitsexperten, die im Rahmen der Cybersicherheit reale Angriffe simuliert. Ihr Ziel ist es, Schwachstellen in der IT-Infrastruktur, bei Mitarbeitern (Social Engineering) und in physischen Sicherheitsvorkehrungen aufzudecken, um die Abwehrmaßnahmen zu verbessern.