

Für eine sichere und widerstandsfähige Stromversorgung

RESILIENZ STÄRKEN

Ein resilientes Stromsystem braucht klare Zuständigkeiten, wirksamen Schutz, sichere Lieferketten und einen verlässlichen Finanzierungsrahmen.

Oktober 2026, Version 1.0

Inhalt

I. Kernforderungen im Überblick	2
1. Einordnung und Grundverständnis	5
2. Politischer Handlungsbedarf.....	6
2.1 KRITIS-Dachgesetz und resilienzorientierter Rechtsrahmen.....	6
2.2 Transparenz, Daten- und Informationsschutz.....	7
2.3 Rollen, Zuständigkeit und Zusammenarbeit	8
2.4 Finanzierung und regulatorische Rahmenbedingungen	9
3. Operative Resilienzfelder.....	10
3.1 Physische Resilienz.....	10
3.2 Materialverfügbarkeit und Lieferketten.....	13
3.3 Technologie und System- und digitale Resilienz	14
4. Personelle Resilienz	16

I. Kernforderungen im Überblick

Governance, Rechtsrahmen und staatliche Verantwortung

- / Resilienz als gesamtgesellschaftliche Aufgabe institutionell verankern und die Zusammenarbeit von Staat, Betreibern kritischer Infrastrukturen und weiteren relevanten Akteuren systematisch stärken.
- / Anforderungen des KRITIS-Dachgesetzes konkretisieren und praxistauglich ausgestalten, insbesondere bei Risikoanalysen, Resilienzplänen und deren Umsetzung im Netzbetrieb.
- / Verantwortlichkeiten, Zuständigkeiten und Entscheidungswege zwischen Staat, Sicherheits-behörden und Betreibern kritischer Infrastrukturen eindeutig festlegen und transparent ausgestalten.
- / KRITIS-Dachgesetz, NIS2 und weitere sektorale Vorgaben stärker harmonisieren, um Doppelstrukturen, Mehrfachnachweise und unnötigen Verwaltungsaufwand zu vermeiden.
- / Einen dauerhaften, strukturierten und bidirektionalen Informationsaustausch zwischen staatlichen Stellen und Betreibern kritischer Infrastrukturen institutionell verankern sowie klare Kontaktstellen, Eskalations-wege und Kommunikationsprozesse für Krisen- und Gefahrenlagen schaffen.
- / Regelmäßige sektorübergreifende Übungen, gemeinsame Notfallplanungen und Krisenformate zwischen Staat, Behörden und Betreibern kritischer Infrastrukturen etablieren und dauerhaft mit ausreichenden personellen und organisatorischen Ressourcen hinterlegen.

Informationsschutz und Datenschutz

- / Bestehende Transparenz- und Veröffentlichungspflichten regelmäßig auf ihre Sicherheitsrelevanz und Verhältnismäßigkeit überprüfen sowie den Informationsschutz im KRITIS-Bereich durch stärkere Berücksichtigung des Need-to-know-Prinzips und der Kumulationswirkung von Informationen stärken.
- / Praxistaugliche Rechtsgrundlagen schaffen, die wirksame Sicherheitsmaßnahmen im KRITIS-Bereich ermöglichen und Datenschutz sowie den Schutz kritischer Infrastrukturen in einen angemessenen Ausgleich bringen.

Finanzierung, Regulierung und Netzplanung

- / Geeignete regulatorische und finanzielle Rahmenbedingungen schaffen, um Investitionen in die Resilienz kritischer Infrastrukturen langfristig zu ermöglichen.
- / Resilienz als eigenständigen Bewertungsmaßstab in Regulierung und Netzplanung neben klassischen Effizienzkriterien verankern.
- / Verbindliche und verlässliche Refinanzierungsmechanismen schaffen sowie CAPEX- und OPEX-Kosten für resilienzrelevante Investitionen, Sicherheitsmaßnahmen und Krisenvorsorge vollständig und ohne Zeitverzug anerkennen.
- / Regulatorische Anreize und geeignete Förderinstrumente für Innovationen im Bereich Resilienz schaffen.

- / Für Resilienzmaßnahmen mit gesamtgesellschaftlichem, sicherheitspolitischem oder staatlichem Nutzen ergänzende staatliche Finanzierungsinstrumente prüfen und eine faire Verteilung der Kosten sicherstellen.

Schutz, Wiederherstellung und Krisenfähigkeit

- / Schutz- und Härtingsmaßnahmen an kritischen Infrastrukturen durch praxistaugliche und unbürokratische Genehmigungs- und Umsetzungsverfahren erleichtern.
- / Resilienzanforderungen stärker in der Netzplanung berücksichtigen und zusätzliche Spielräume für geo-redundante Lösungen bei besonders kritischen Netzelementen schaffen.
- / Rechtliche und organisatorische Rahmenbedingungen schaffen, die eine schnelle Wiederherstellung kritischer Infrastrukturen ermöglichen, einschließlich klarer Regelungen für Flächenzugang, Transport-, Genehmigungs- und Wiederherstellungsmaßnahmen im Havarie- und Krisenfall.
- / Drohnenvorfälle an kritischen Infrastrukturen durch klare Zuständigkeiten, verlässliche staatliche Reaktionsstrukturen, rechtssichere Möglichkeiten zur Lageerkennung sowie eine enge Zusammenarbeit von Betreibern, Sicherheitsbehörden und dem Gemeinsamen Drohnenabwehrzentrum adressieren.
- / Sicherstellen, dass Betreiber kritischer Infrastrukturen auch im Spannungs-, Verteidigungs- oder Bündnisfall ihre Anlagen erreichen, instandsetzen und betreiben können.

Lieferketten, Industrie und strategische Reserven

- / Strategische Abhängigkeiten von Drittstaaten bei kritischen Komponenten reduzieren und die Versorgungssicherheit bei sicherheitsrelevanten Betriebsmitteln stärken.
- / Produktions-, Wartungs- und Instandsetzungskapazitäten für kritische Netzkomponenten in Europa gezielt stärken und absichern.
- / Regulatorische Rahmenbedingungen schaffen, die den Aufbau resilienzrelevanter Lager-, Reserve- und Bevorratungskonzepte ermöglichen sowie gemeinsame nationale oder europäische Reserve- und Unterstützungskonzepte für besonders kritische Betriebsmittel prüfen.
- / Regulatorische und beschaffungsrechtliche Vorgaben so ausgestalten, dass sie die Resilienz von Lieferketten stärken und die Verfügbarkeit kritischer Komponenten nicht unnötig beeinträchtigen.
- / Stromnetze und kritische Netztechnologien von zusätzlichen Beschaffungsvorgaben ausnehmen, die den rechtzeitigen Aus- und Umbau der Energieinfrastruktur gefährden können.

Digitalisierung, Systemstabilität und technologische Souveränität

- / Verbindliche Sicherheits- und Resilienzanforderungen für systemrelevante Komponenten und neue Marktteilnehmer wie Speicher, Wechselrichter, Elektrolyseure und Aggregatoren schaffen.
- / Die Steuerbarkeit und Beobachtbarkeit dezentraler Erzeugungs- und Speicheranlagen sicherstellen und den Rollout intelligenter Messsysteme beschleunigen.
- / Digitale Souveränität stärken und technologische Abhängigkeiten von außereuropäischen Hard- und Software-, Cloud- und Plattformanbietern reduzieren.

- / Technische Standards, Sicherheitsanforderungen und regulatorische Vorgaben für Resilienz europaweit stärker harmonisieren.

Klimaresilienz und Klimaanpassung

- / Einheitliche europäische Standards für Klimarisikoanalysen schaffen sowie nationale Klimaresilienzpläne etablieren.
- / Klimaresilienzmaßnahmen von Übertragungsnetzbetreibern regulatorisch vollständig anerkennen und refinanzieren.
- / Klimarisiken stärker in Flächennutzungs- und Planungsprozessen berücksichtigen, ohne die Umsetzung kritischer Infrastrukturvorhaben unverhältnismäßig zu erschweren.
- / Dem Netzausbau als Voraussetzung für Energiewende, Versorgungssicherheit und Klimaschutz einen ausdrücklichen Vorrang im Planungs- und Genehmigungsrecht einräumen.

Personelle Resilienz

- / Datenschutzrechtliche und organisatorische Rahmenbedingungen so ausgestalten, dass Sicherheitsüberprüfungen für Mitarbeitende in sicherheitsrelevanten KRITIS-Funktionen wirksam, verhältnismäßig und unbürokratisch durchgeführt werden können.
- / Behördliche Sicherheitsüberprüfungs- und Informationsprozesse stärker digitalisieren und die zuständigen Behörden personell stärken, um Verfahren zu beschleunigen und die Besetzung sicherheitsrelevanter Positionen zu erleichtern.
- / Ausbildung, Qualifizierung und Gewinnung von Fachkräften in KRITIS-relevanten Berufen gezielt fördern und unterstützen.

1. Einordnung und Grundverständnis

Die europäische Sicherheitslage hat sich in den vergangenen Jahren spürbar verändert. Geopolitische Spannungen, hybride Bedrohungen, Cyberangriffe sowie zunehmend häufige Extremwetterereignisse rücken die Resilienz kritischer Infrastrukturen stärker in den Fokus. Dem Energiesystem kommt dabei eine besondere Bedeutung zu, da es die Grundlage für das Funktionieren nahezu aller gesellschaftlichen und wirtschaftlichen Bereiche bildet.

Resilienz beschreibt die Fähigkeit kritischer Infrastrukturen, Funktionen auch unter Störungen aufrechtzuerhalten, Beeinträchtigungen zu überwinden und sich an veränderte technische, klimatische und gesellschaftliche Rahmenbedingungen anzupassen. Dieses Verständnis orientiert sich an der Resilienzdefinition des VDE. Dabei hängt die Widerstandsfähigkeit des Stromsystems nicht allein von der Netzinfrastruktur ab, sondern gleichermaßen von funktionsfähigen Abhängigkeiten zu Wasser-, Telekommunikations-, IT-, Verkehrs- und Verwaltungsstrukturen. Resilienz geht über den Schutz bestehender Anlagen hinaus. Sie umfasst insbesondere die Fähigkeit, kritische Funktionen nach einem Störfall rasch wiederherzustellen, und schließt dabei auch Leit- und Kommunikationssysteme, personelle Ressourcen sowie robuste Lieferketten ein.

Absolute Sicherheit ist dabei weder realistisch noch wirtschaftlich sinnvoll; entscheidend ist ein professioneller Umgang mit Restrisiken und eine ausgewogene Balance zwischen Resilienzniveau, Kosten und gesellschaftlichen Erwartungen. Im Mittelpunkt sollten die drei Leitprinzipien Robustheit, Erholungsfähigkeit und Anpassungsfähigkeit stehen.

Während der operative Schutz kritischer Infrastrukturen, insbesondere die physische Sicherheit, Gefahrenabwehr und Krisenbewältigung, in der Verantwortung der europäischen Mitgliedstaaten bleibt, haben Sicherheitsdefizite aufgrund der grenzüberschreitenden Vernetzung der Energiesysteme potenziell direkte Auswirkungen auf Nachbarländer. Daher besteht ein berechtigtes europäisches Interesse, die Resilienz kritischer Infrastrukturen durch gemeinsame Mindeststandards, Unterstützung und koordinierte Maßnahmen zu stärken.

Die Resilienz kritischer Infrastrukturen kann dabei nur im Zusammenspiel von Staat, Betreibern kritischer Einrichtungen und weiteren gesellschaftlichen Akteuren wirksam gestärkt werden und ist daher als gesamtgesellschaftliche Aufgabe zu verstehen.

Herausforderungen und Chancen für das Stromsystem

Die Anforderungen an die Resilienz des Stromnetzes nehmen kontinuierlich zu. Neben klassischen Risiken müssen Übertragungsnetzbetreiber heute einen **All-Gefahren-Ansatz** verfolgen, der Naturereignisse und Extremwetter, technische Störungen und Systemausfälle, Cyberangriffe, Sabotageakte, hybride Bedrohungen sowie die Auswirkungen geopolitischer Spannungen gleichermaßen berücksichtigt. Die Transformation des Energiesystems schafft erhebliche Chancen für Klimaschutz, Wertschöpfung und die Resilienz der Energieversorgung.

Eine stärkere Diversifizierung der Erzeugungsstruktur, die zunehmende Nutzung heimischer erneuerbarer Energien sowie neue Flexibilitätsoptionen können dazu beitragen, Abhängigkeiten zu reduzieren und die Widerstandsfähigkeit des Energiesystems zu stärken. Gleichzeitig verringert der Ausbau heimischer Energiequellen die Abhängigkeit von importierten Energieträgern und erhöht damit die Robustheit gegenüber geopolitischen Krisen, internationalen Lieferengpässen und Störungen globaler Handelswege. Gleichzeitig erhöht die Transformation die Komplexität des Netzbetriebs. Mit der zunehmenden Integration erneuerbarer Energien, Speichern und neuer Marktteilnehmer müssen essenzielle Systemdienstleistungen und die Steuerbarkeit von Leistungsflüssen auch künftig zuverlässig gewährleistet werden. Darüber hinaus wirken sich klimabedingte Extremereignisse wie Hitze, Trockenheit, Hochwasser, Stürme oder Eislasten zunehmend auf die Infrastruktur aus und erfordern angepasste Planungs-, Bau- und Betriebskonzepte.

Die Stärkung der Resilienz setzt daher einen ganzheitlichen Ansatz voraus, der technische, organisatorische und regulatorische Aspekte gleichermaßen adressiert und durch geeignete Investitions- und Finanzierungsrahmen flankiert wird.

2. Politischer Handlungsbedarf

Die steigende Bedrohungslage, die zunehmende Komplexität des Energiesystems sowie die wachsende Bedeutung kritischer Infrastrukturen für Wirtschaft, Gesellschaft und staatliche Handlungsfähigkeit erfordern eine Weiterentwicklung der politischen und regulatorischen Rahmenbedingungen. Resilienz lässt sich nicht allein durch Maßnahmen der Betreiber erreichen, sondern setzt ein abgestimmtes Zusammenspiel von Staat, Behörden und Betreibern voraus. Neben klaren Verantwortlichkeiten und praktikablen gesetzlichen Vorgaben bedarf es geeigneter Rahmenbedingungen für Informationsaustausch, Krisenvorsorge, Finanzierung und die Umsetzung Resilienz-steigernder Maßnahmen. Die folgenden Handlungsfelder zeigen auf, wo aus Sicht der Übertragungsnetzbetreiber besonderer politischer und regulatorischer Anpassungsbedarf besteht.

2.1 KRITIS-Dachgesetz und resilienzorientierter Rechtsrahmen

Mit dem KRITIS-Dachgesetz wird erstmals ein sektorübergreifender Rechtsrahmen für die physische Resilienz kritischer Infrastrukturen geschaffen. Der verpflichtende All-Gefahren-Ansatz stellt dabei einen wichtigen Schritt dar, um Risiken ganzheitlich zu betrachten und Resilienz systematisch zu stärken. Gleichzeitig zeigt die praktische Umsetzung bereits heute, dass zahlreiche Anforderungen einer weiteren Konkretisierung bedürfen. Dies betrifft insbesondere die Ausgestaltung von Risikoanalysen und Resilienzplänen, die Rollenverteilung zwischen Staat und Betreibern kritischer Infrastrukturen sowie die praktische Umsetzung der gesetzlichen Vorgaben im Netzbetrieb. In der Praxis bestehen insbesondere bei der Bereitstellung belastbarer Lagebilder sowie bei der Abgrenzung von Zuständigkeiten und Handlungsmöglichkeiten weiterhin Unklarheiten. Dies zeigt sich beispielsweise bei der Bewertung neuer Bedrohungslagen oder bei Fragen der Lageerkennung und Reaktion auf Drohenvorfälle.

Für Betreiber kritischer Infrastrukturen sind belastbare staatliche Risikoanalysen eine wesentliche Grundlage. Je präziser Bedrohungslagen, Lastannahmen und Schutzanforderungen durch staatliche Stellen beschrieben werden, desto zielgerichteter können Betreiber eigene Risikoanalysen, Resilienzpläne und Schutzkonzepte entwickeln. Gleichzeitig bedarf es klarer Vorgaben, welche Inhalte Resilienzpläne und zugehörige Maßnahmenpakete künftig umfassen sollen. Derzeit bestehen hierfür noch erhebliche Interpretationsspielräume.

Darüber hinaus sollte frühzeitig Klarheit darüber geschaffen werden, welche Risiken und Bedrohungsszenarien durch Betreiber zu adressieren sind und in welchen Fällen staatliche Stellen die Verantwortung übernehmen. Der gesetzliche All-Gefahren-Ansatz darf nicht dazu führen, dass Anforderungen formuliert werden, die außerhalb der tatsächlichen Einfluss- und Handlungsmöglichkeiten kritischer Infrastrukturbetreiber liegen. Resilienz ist eine gemeinsame Aufgabe von Staat und Betreibern und setzt eine klare Abgrenzung von Verantwortlichkeiten, Pflichten und den jeweils erforderlichen Befugnissen voraus.

Angesichts der Größe und der räumlichen Verteilung der Stromnetzinfrastruktur sind der flächendeckenden physischen Sicherung natürliche Grenzen gesetzt. Ein resilienzorientierter Rechtsrahmen sollte daher risikobasierte Ansätze ermöglichen und die Priorisierung besonders kritischer Anlagen und Funktionen unterstützen.

Gleichzeitig bestehen in einzelnen Resilienzbereichen praktische Handlungslücken. Betreiber kritischer Infrastrukturen sind verpflichtet, Risiken zu identifizieren und Schutzmaßnahmen zu ergreifen, verfügen in bestimmten Szenarien jedoch nicht über die erforderlichen Eingriffs- oder Handlungsmöglichkeiten. Der Gesetzgeber sollte daher prüfen, ob bestehende Zuständigkeiten und Befugnisse ausreichend sind, um identifizierte Risiken wirksam adressieren zu können.

Die Umsetzung des KRITIS-Dachgesetzes sollte eng mit bestehenden Anforderungen aus anderen Regelwerken abgestimmt werden. Insbesondere Überschneidungen mit NIS2 und weiteren sektoralen Vorgaben sollten vermieden werden, um Doppelstrukturen, Mehrfachnachweise und unnötigen Verwaltungsaufwand zu

verhindern. Ziel sollte ein kohärenter und praktikabler Resilienzrahmen sein, der bestehende Anforderungen sinnvoll ergänzt und nicht mehrfach dieselben Sachverhalte reguliert.

Schließlich bedarf es einer raschen Konkretisierung der Rolle des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zuständige Aufsicht. Für die betroffenen Betreiber muss transparent sein, anhand welcher Maßstäbe die Umsetzung der gesetzlichen Anforderungen künftig überprüft wird und welche Erwartungen an Nachweise, Risikoanalysen und Resilienzkonzepte gestellt werden. Ebenso sollten Fragen des Business Continuity Managements (BCM) und dessen Verhältnis zu den neuen gesetzlichen Anforderungen frühzeitig geklärt werden, um Planungssicherheit für die Umsetzung zu schaffen.

2.2 Transparenz, Daten- und Informationsschutz

Transparenz ist ein wesentlicher Bestandteil eines funktionierenden Energiemarktes und ermöglicht die regulatorische Aufsicht sowie die Nachvollziehbarkeit zentraler Markt- und Netzprozesse. Gleichzeitig hat sich das sicherheitspolitische Umfeld in den vergangenen Jahren deutlich verändert. Vor diesem Hintergrund sollte überprüft werden, ob bestehende Transparenz- und Veröffentlichungspflichten weiterhin in ihrem heutigen Umfang erforderlich und verhältnismäßig sind.

Viele der bestehenden Vorgaben wurden zu einer Zeit geschaffen, in der Markttransparenz und die möglichst umfassende Bereitstellung von Informationen im Vordergrund standen. Heute stellt sich zunehmend die Frage, ob einzelne Veröffentlichungen unbeabsichtigt Rückschlüsse auf kritische Infrastrukturen, betriebliche Abläufe oder potenzielle Schwachstellen ermöglichen. Dies betrifft insbesondere Informationen, die eine räumliche Zuordnung kritischer Netzelemente erlauben oder Hinweise auf Belastungssituationen und betriebliche Einschränkungen im Netz geben können.

Ziel sollte dabei nicht sein, Transparenz grundsätzlich in Frage zu stellen. Vielmehr bedarf es einer ausgewogenen Balance zwischen Transparenzinteressen, regulatorischen Anforderungen und dem Schutz kritischer Infrastrukturen. Regulatorische Aufsicht und Markttransparenz müssen weiterhin gewährleistet bleiben, ohne durch übermäßige Berichtspflichten sensible betriebliche und infrastrukturelle Informationen offenzulegen.

Dabei sollte die Betrachtung nicht auf einzelne Veröffentlichungspflichten beschränkt bleiben. Sicherheitsrisiken entstehen häufig erst durch die Verknüpfung verschiedener Datenquellen. Informationen, die für sich genommen unkritisch erscheinen, können in ihrer Gesamtheit ein detailliertes Lagebild über kritische Infrastrukturen, Betriebszustände oder potenzielle Verwundbarkeiten ermöglichen. Entsprechend sollten Sicherheitsbewertungen künftig stärker die Kumulationswirkung verschiedener Veröffentlichungen berücksichtigen.

Sicherheitsrelevante Informationen sollten darüber hinaus stärker nach dem Need-to-know-Prinzip bereitgestellt werden. Der Zugang zu sensiblen Informationen sollte auf diejenigen Akteure beschränkt werden, die diese Informationen tatsächlich für die Erfüllung ihrer Aufgaben benötigen. Dadurch lassen sich Transparenzanforderungen und Informationsschutz besser in Einklang bringen und unnötige Sicherheitsrisiken vermeiden.

Angesichts der veränderten Bedrohungslage sollten bestehende Transparenz- und Veröffentlichungspflichten regelmäßig auf ihre Sicherheitsrelevanz und Verhältnismäßigkeit überprüft werden. Dies gilt insbesondere für Vorgaben, die eine Lokalisation kritischer Netzelemente ermöglichen oder Rückschlüsse auf Netzbelastungen, Engpässe oder betriebliche Schwachstellen zulassen. Eine detaillierte Analyse möglicher Veröffentlichungspflichten und ihrer sicherheitsrelevanten Auswirkungen sollte hierbei als Grundlage für die weitere Bewertung dienen. Dies sollte auch für Veröffentlichungspflichten gelten, die im Rahmen politischer Beteiligungs- und Konsultationsverfahren entstehen. Stellungnahmen und Gutachten von Betreibern kritischer Infrastrukturen enthalten häufig Informationen zu Verwundbarkeiten, Sicherheitsanforderungen, Schutzmaßnahmen oder regulatorischen Handlungsbedarfen. Auch wenn einzelne Informationen geschwärzt werden können, kann bereits die Gesamtschau eines Dokuments sicherheitsrelevante Rückschlüsse ermöglichen. Daher sollte

geprüft werden, ob bestehende Veröffentlichungspflichten den besonderen Schutzanforderungen kritischer Infrastrukturen ausreichend Rechnung tragen und für sicherheitsrelevante Inhalte weitergehende Vertraulichkeitsregelungen erforderlich sind.

Eng mit dieser Fragestellung verbunden ist der Umgang mit Datenschutzanforderungen im KRITIS-Bereich. Betreiber kritischer Infrastrukturen müssen in der Lage sein, angemessene und wirksame Sicherheitsmaßnahmen rechtssicher umzusetzen. Dies betrifft beispielsweise Videoüberwachung, Zugangskontrollen, die Erstellung von Lagebildern oder den Austausch sicherheitsrelevanter Informationen. Der bestehende Datenschutzrahmen sollte daher daraufhin überprüft werden, ob er den besonderen Schutzanforderungen kritischer Infrastrukturen ausreichend Rechnung trägt. Wo erforderlich, sollten klare und praxistaugliche Rechtsgrundlagen geschaffen werden, die sowohl den Schutz personenbezogener Daten als auch die wirksame Sicherung kritischer Infrastrukturen gewährleisten.

2.3 Rollen, Zuständigkeit und Zusammenarbeit

Die Resilienz kritischer Energieinfrastrukturen setzt ein verlässliches Zusammenspiel von Staat, Behörden und Betreibern voraus. Übertragungsnetzbetreiber können durch Prävention, Schutzmaßnahmen, Risikoanalysen, Lagebewertung und Krisenvorsorge einen wesentlichen Beitrag zur Sicherheit des Stromsystems leisten. Zugleich darf mit steigenden Resilienzanforderungen keine schleichende Verlagerung hoheitlicher Sicherheits- und Gefahrenabwehraufgaben auf private Betreiber einhergehen. Die Verantwortung für Gefahrenabwehr, staatlichen Schutz und sicherheitsbehördliche Bewertung muss klar definiert und beim Staat verankert bleiben. Betreiber können Risiken identifizieren, Schutzmaßnahmen umsetzen und die Resilienz ihrer Infrastruktur stärken, sie können staatliche Sicherheitsaufgaben jedoch nicht ersetzen.

Gerade in Krisen- und Gefahrenlagen braucht es eindeutige Rollen, Zuständigkeiten und Entscheidungswege. Für Betreiber kritischer Infrastrukturen muss klar sein, welche staatliche Stelle in welcher Lage zuständig ist, wer koordiniert, wer entscheidet und welche Unterstützung im Ereignisfall konkret zur Verfügung steht. Dies betrifft sowohl akute Krisensituationen als auch die vorbereitende Lagebewertung, Prävention, gemeinsame Krisenvorsorge und Intervention. Unklare Verantwortlichkeiten können im Ernstfall zu Zeitverlusten führen und die Wirksamkeit von Schutz- und Wiederherstellungsmaßnahmen erheblich beeinträchtigen.

Ein zentraler Baustein ist ein verlässlicher, bidirektionaler Informationsfluss zwischen Behörden und Betreibern. Betreiber sind auf zeitnahe und nutzbare Informationen zur Bedrohungslage angewiesen, um Risiken einordnen und angemessene Schutz- oder Vorsorgemaßnahmen treffen zu können. Umgekehrt verfügen Betreiber über detaillierte Kenntnisse ihrer Anlagen, Systeme und Betriebsabläufe, die für staatliche Lagebilder und Krisenbewertungen von hoher Bedeutung sein können. Dieser Austausch sollte nicht erst im Krisenfall erfolgen, sondern als dauerhafter Regelfall institutionell verankert werden.

Dazu gehören klare Kontaktstellen, definierte Eskalationswege und abgestimmte Kommunikationsprozesse. Aus Sicht der Betreiber ist entscheidend, dass im Not- oder Krisenfall schnell erkennbar ist, welche Stelle erreichbar ist, welche Informationen benötigt werden und welche Maßnahmen durch wen veranlasst werden können. Die Zusammenarbeit darf nicht von gewachsenen Einzelkontakten abhängen, sondern sollte strukturiert, belastbar und dauerhaft etabliert sein.

Dies gilt insbesondere im Zusammenspiel mit Polizei, Verfassungsschutz, Katastrophenschutz- und Zivilschutzbehörden sowie weiteren zuständigen Sicherheitsbehörden. Auch kommunale und regionale Akteure wie Feuerwehren, Katastrophenschutzbehörden, Landratsämter oder Regierungspräsidien spielen insbesondere bei Havarien, Wiederherstellungsmaßnahmen und Krisenlagen eine wichtige Rolle. Die Bundeswehr kann darüber hinaus in sicherheits- und verteidigungspolitischen Krisenlagen, insbesondere im Rahmen der Gesamtverteidigung und des Operationsplans Deutschland, ein relevanter Partner sein. Für Betreiber kritischer Infrastrukturen muss nachvollziehbar sein, welche Aufgaben die jeweiligen Akteure wahrnehmen und welche Unterstützung im Ereignisfall konkret zur Verfügung steht.

Neben klaren Zuständigkeiten und Kommunikationswegen braucht es eine stärkere gemeinsame Vorbereitung auf Krisenlagen. Regelmäßige Übungen, Planspiele und gemeinsame Krisenformate zwischen Staat,

Behörden, Sicherheitskräften und Betreibern können dazu beitragen, Zuständigkeiten, Informationsflüsse und Entscheidungsprozesse bereits vor einem Ereignisfall zu erproben. Dabei sollte die gemeinsame Vorbereitung auf Krisenlagen auch die Einbindung von Polizei, Bundeswehr und weiteren sicherheitsrelevanten Akteuren umfassen, um die Zusammenarbeit unter realistischen Bedingungen zu trainieren. Gerade bei kritischen Energieinfrastrukturen reicht es nicht aus, Verantwortlichkeiten abstrakt zu beschreiben. Entscheidend ist, dass die Zusammenarbeit im Ereignisfall praktisch funktioniert und die beteiligten Stellen ihre jeweiligen Rollen kennen. Eine wirksame Krisenvorsorge setzt daher voraus, dass Übungen und Vorbereitungsmaßnahmen dauerhaft mit ausreichenden personellen, organisatorischen und zeitlichen Ressourcen hinterlegt werden. Dabei sollten auch sektorübergreifende Abhängigkeiten sowie mögliche Kaskaden- und Mehrfachausfälle berücksichtigt werden. Krisenszenarien betreffen häufig nicht nur die Stromversorgung, sondern gleichzeitig weitere kritische Infrastrukturen wie Telekommunikation, Verkehr, Wasser oder Verwaltung. Eine wirksame Krisenvorsorge erfordert daher gemeinsame Notfallplanungen und regelmäßige Übungen über Sektor- und Organisationsgrenzen hinweg, einschließlich komplexer und hybrider Krisenszenarien.

Ziel muss eine institutionalisierte Zusammenarbeit sein, die Lagefeststellung, Prävention, Krisenreaktion, Intervention und Wiederherstellung zusammendenkt. Betreiber kritischer Infrastrukturen benötigen hierfür keine Übertragung hoheitlicher Befugnisse, sondern einen klaren staatlichen Ordnungsrahmen, verlässliche Ansprechpartner und wirksame Unterstützungsstrukturen. Nur so lässt sich sicherstellen, dass betriebliche Vorsorge und staatliche Gefahrenabwehr wirksam ineinandergreifen, ohne Verantwortlichkeiten zu verwischen.

2.4 Finanzierung und regulatorische Rahmenbedingungen

Die Anforderungen an die Resilienz kritischer Energieinfrastrukturen steigen kontinuierlich. Der bestehende Regulierungsrahmen ist jedoch weiterhin stark auf die möglichst effiziente Bereitstellung netzbetrieblicher Leistungen ausgerichtet. Zukünftige Bedrohungen und die wachsende Bedeutung von Sicherheit, Vorsorge und Krisenfestigkeit erfordern eine stärkere Berücksichtigung von Resilienzaspekten in Regulierung und Finanzierung. Resilienzmaßnahmen dürfen nicht ausschließlich unter klassischen Effizienzmaßstäben bewertet, sondern müssen zusätzlich unter Sicherheits-, Vorsorge- und Versorgungsgesichtspunkten betrachtet werden.

Der regulatorische Effizienzbegriff orientiert sich heute primär an betriebswirtschaftlichen Kosten. Für die Bewertung von Resilienzmaßnahmen greift diese Betrachtung jedoch häufig zu kurz. Resilienzmaßnahmen dienen gerade dazu, seltene, aber potenziell schwerwiegende Ereignisse zu vermeiden oder deren Auswirkungen zu begrenzen. Ihre Wirtschaftlichkeit bemisst sich daher nicht allein an den unmittelbaren Kosten einer Maßnahme, sondern auch an der Eintrittswahrscheinlichkeit von Risiken, dem potenziellen Schadensausmaß sowie den vermiedenen volkswirtschaftlichen, sicherheits- und gesellschaftspolitischen Folgekosten. Eine Maßnahme kann aus betriebswirtschaftlicher Sicht zusätzliche Kosten verursachen und gleichzeitig aus gesamtwirtschaftlicher Perspektive hoch effizient sein, wenn sie das Risiko schwerwiegender Versorgungsunterbrechungen reduziert. Diese Zusammenhänge sollten künftig stärker im regulatorischen Rahmen berücksichtigt werden.

Dies betrifft auch die Netzplanung. Die derzeitigen Planungsgrundsätze sind stark auf Effizienz, Bündelung und die Minimierung des Netzausbaubedarfs ausgerichtet. Aus Resilienzsicht kann es jedoch sinnvoll sein, zusätzliche Redundanzen, geo-redundante Strukturen oder begrenzte Leistungsreserven vorzusehen, um die Auswirkungen von Extremereignissen, technischen Störungen oder gezielten Angriffen zu begrenzen. Resilienz sollte deshalb als eigenständiger Bewertungsmaßstab neben klassischen Effizienzüberlegungen berücksichtigt werden. Dabei gilt es insbesondere zu prüfen, wie kritische Verwundbarkeiten durch räumliche Konzentrationen oder gemeinsame Fehlerursachen reduziert werden können, ohne die Grundsätze einer wirtschaftlichen Netzplanung grundsätzlich in Frage zu stellen.

Resilienz erfordert zusätzliche Investitionen in Infrastruktur, Technologien, Personal und organisatorische Fähigkeiten. Dazu gehören beispielsweise der Aufbau von Redundanzen, die Vorhaltung kritischer Ressourcen, die Verbesserung von Schutzmaßnahmen, die Stärkung von Krisen- und Wiederherstellungsfähigkeiten sowie

die Entwicklung neuer technischer und organisatorischer Lösungen. Diese Maßnahmen erhöhen kurzfristig die Kostenbasis, reduzieren jedoch langfristig systemische Risiken und tragen dazu bei, erhebliche volkswirtschaftliche Schäden sowie Beeinträchtigungen der Versorgungssicherheit zu vermeiden.

Für Betreiber kritischer Infrastrukturen sind daher langfristige Planungssicherheit, regulatorische Verlässlichkeit und klare Anerkennungsmaßstäbe von zentraler Bedeutung. Neue Resilienzanforderungen sollten grundsätzlich mit einer verbindlichen Regelung zur Refinanzierung verbunden werden. Erforderlich sind transparente und praktikable Kriterien, welche Maßnahmen als resilienzrelevant gelten und unter welchen Voraussetzungen ihre Kosten regulatorisch anerkannt werden. Dabei können branchenspezifische Resilienzstandards oder staatlich definierte Schutzanforderungen eine wichtige Grundlage schaffen. Wenn bestimmte Resilienzmaßnahmen regulatorisch oder staatlich vorgegeben werden, sollte deren Anerkennung und Refinanzierung verbindlich sichergestellt werden.

Resilienzmaßnahmen verursachen sowohl kapitalintensive Investitionen als auch dauerhaft anfallende Betriebs-, Personal- und Vorhaltekosten. Viele dieser Maßnahmen entfalten ihren Nutzen erst im Störungs- oder Krisenfall und lassen sich daher nur eingeschränkt anhand klassischer Effizienzkennzahlen bewerten. Sowohl CAPEX als auch OPEX sollten vollständig, verlässlich und ohne Zeitverzug anerkannt werden können. Dies gilt insbesondere für dauerhaft erforderliche Sicherheits-, Vorsorge- und Krisenmanagementmaßnahmen, die zu zusätzlichen laufenden Aufwendungen führen. Ebenso sollte der regulatorische Rahmen sicherstellen, dass Anlagen, die aufgrund neuer Resilienz- oder Sicherheitsanforderungen vorzeitig ersetzt, erweitert oder angepasst werden müssen, nicht zu wirtschaftlichen Nachteilen für die Betreiber führen. Regulatorische Vorgaben sollten kurze Abschreibungsdauern für sicherheitsrelevante Technologien berücksichtigen, da deren Lebenszyklen aufgrund des raschen technologischen Fortschritts deutlich kürzer sind.

Darüber hinaus sollte die Regulierung Anreize für Innovationen im Bereich Resilienz schaffen. Neue Technologien, Sicherheitskonzepte und Vorsorgemaßnahmen leisten einen wichtigen Beitrag zur langfristigen Widerstandsfähigkeit kritischer Infrastrukturen, können jedoch häufig nicht innerhalb bestehender Effizienzmechanismen abgebildet werden. Geeignete Innovationsbudgets oder vergleichbare Instrumente können dazu beitragen, notwendige Entwicklungen zu beschleunigen.

Gleichzeitig dient Resilienz nicht ausschließlich netzbetrieblichen Zielen. Maßnahmen zum Schutz kritischer Infrastrukturen, zur Vorsorge gegenüber hybriden Bedrohungen oder zur Sicherstellung staatlicher Handlungsfähigkeit verfolgen regelmäßig auch gesamtgesellschaftliche, sicherheits- und staatspolitische Ziele. Vor diesem Hintergrund sollte geprüft werden, ob bestimmte Resilienzmaßnahmen ausschließlich über Netzentgelte finanziert werden sollten oder ergänzende staatliche Finanzierungsinstrumente erforderlich sind. Hierzu können je nach Ausgestaltung auch Fondsmodelle oder andere Formen staatlicher Mitfinanzierung beitragen. Eine faire Verteilung der Kosten ist Voraussetzung dafür, dass die notwendigen Investitionen in die Resilienz kritischer Energieinfrastrukturen dauerhaft umgesetzt werden können.

3. Operative Resilienzfelder

Die Resilienz kritischer Energieinfrastrukturen wird nicht allein durch regulatorische Vorgaben oder organisatorische Strukturen bestimmt. Entscheidend ist, wie resilient das Stromsystem und seine Betreiber im operativen Alltag aufgestellt sind. Dazu gehören der Schutz kritischer Anlagen, die Verfügbarkeit von Materialien und Dienstleistungen, die Beherrschung neuer technologischer Risiken sowie die Fähigkeit, auf Störungen und Krisenlagen wirksam zu reagieren. Die folgenden Handlungsfelder beschreiben zentrale Bausteine einer resilienten Stromnetzinfrastuktur aus Sicht der Übertragungsnetzbetreiber.

3.1 Physische Resilienz

Die physische Resilienz kritischer Energieinfrastrukturen umfasst weit mehr als den Schutz einzelner Anlagen. Ziel ist es, die Funktionsfähigkeit des Stromsystems auch unter außergewöhnlichen Belastungen, gezielten Angriffen oder nach Schadensereignissen aufrechtzuerhalten beziehungsweise schnell wiederherzustellen.

Dies erfordert ein Zusammenspiel aus planerischen, organisatorischen, technischen und baulichen Maßnahmen entlang des gesamten Lebenszyklus kritischer Infrastrukturen. Auch die Auswirkungen des

Klimawandels gewinnen hierbei zunehmend an Bedeutung. Hitzeperioden, Trockenheit, Starkregen, Hochwasser, Stürme oder Eislasten können die Belastung kritischer Infrastrukturen erhöhen und sowohl den Betrieb als auch die Lebensdauer von Anlagen beeinflussen. Physische Resilienz erfordert daher, Klimarisiken systematisch in Planung, Bau, Betrieb und Instandhaltung der Netzinfrastruktur einzubeziehen und entsprechende Anpassungsmaßnahmen frühzeitig vorzusehen.

Ein wirksamer physischer Schutz beginnt bei der systematischen Identifikation und Priorisierung besonders kritischer Anlagen und Funktionen. Aufgrund der Größe und räumlichen Ausdehnung des Übertragungsnetzes ist eine flächendeckende Sicherung aller Assets weder technisch noch wirtschaftlich realisierbar. Daher sollte der Fokus auf risikobasierten Schutzkonzepten liegen, die insbesondere die Schutzfunktionen Abschreckung, Detektion, Verzögerung, Verifikation und Reaktion berücksichtigen. Physische Resilienz erfordert dabei nicht nur klassische Objektschutzmaßnahmen wie Zäune, Zugangskontrollen oder Überwachungssysteme, sondern auch eine kontinuierliche Bewertung von Verwundbarkeiten und potenziellen Angriffspfaden.

Neben klassischen Schutzmaßnahmen kommt der Möglichkeit, Schutz- und Härtungsmaßnahmen an kritischen Anlagen schnell und rechtssicher umzusetzen, eine wachsende Bedeutung zu. Resilienzmaßnahmen sollten dort, wo sie ausschließlich der Erhöhung des Schutzniveaus dienen, möglichst unbürokratisch umsetzbar sein. Dies gilt insbesondere vor dem Hintergrund einer verschärften Sicherheitslage und zunehmender Anforderungen an den Schutz kritischer Infrastrukturen.

Besondere Aufmerksamkeit verdienen sogenannte Single Points of Failure, deren Ausfall erhebliche Auswirkungen auf die Versorgungssicherheit haben kann. Dies betrifft beispielsweise räumliche Bündelungen von Leitungen oder andere Infrastrukturelemente mit hoher Systemrelevanz. Wo einzelne Anlagen oder räumliche Konzentrationen von Betriebsmitteln besondere Verwundbarkeiten erzeugen, sollte geprüft werden, wie diese Risiken durch geeignete planerische, technische oder organisatorische Maßnahmen reduziert werden können. Neben klassischen Redundanzen können hierbei auch alternative Netzstrukturen, geo-redundante Lösungen oder Wiederherstellungskonzepte eine Rolle spielen. Neben gezielten Angriffen können auch Naturereignisse, technische Störungen oder sogenannte Common-Mode-Fehler mehrere kritische Betriebsmittel gleichzeitig beeinträchtigen. Bestehende Planungsgrundsätze führen teilweise dazu, dass mehrere systemrelevante Netzelemente aufgrund von Effizienz- und Bündelungsanforderungen räumlich konzentriert werden. Aus Resilienz-sicht sollte daher geprüft werden, ob für besonders kritische Netzelemente zusätzliche Spielräume für geo-redundante Lösungen geschaffen werden können, um die Auswirkungen von Extremwetterereignissen, Wartungszuständen oder gezielten Eingriffen zu begrenzen. Dies gilt insbesondere vor dem Hintergrund eines zunehmend ausgelasteten und im Umbau befindlichen Energiesystems, in dem geplante Außerbetriebnahmen einzelner Betriebsmittel im Rahmen von Umbau-, Wartungs- oder Instandhaltungsmaßnahmen die Verwundbarkeit gegenüber zusätzlichen Störungen erhöhen können.

Neben präventiven Schutzmaßnahmen kommt der Fähigkeit zur schnellen Wiederherstellung des Netzbetriebs eine zentrale Bedeutung zu. Die Erfahrungen der vergangenen Jahre zeigen, dass kritische Infrastrukturen selbst bei hohen Sicherheitsstandards nicht vollständig vor Naturereignissen, technischen Störungen oder gezielten Angriffen geschützt werden können. Entscheidend ist daher nicht allein die Vermeidung von Schäden, sondern die Fähigkeit, Auswirkungen zu begrenzen, Schäden rasch zu beheben und die Versorgung schnellstmöglich wiederherzustellen. Die physische Resilienz des Stromnetzes bemisst sich damit nicht nur an seiner Widerstandsfähigkeit, sondern gleichermaßen an seiner Reaktions- und Wiederherstellungsfähigkeit.

Hierfür sind Havariekonzepte, Notfallprozesse, Materialreserven und vorbereitete Wiederherstellungsmaßnahmen von zentraler Bedeutung. Gleichzeitig sollten die rechtlichen Rahmenbedingungen sicherstellen, dass im Krisen- oder Schadensfall schnell gehandelt werden kann. Dies betrifft beispielsweise Genehmigungen für Provisorien und Ersatzbauwerke, Transportmöglichkeiten, Flächennutzungen oder sonstige Maßnahmen, die für eine zügige Wiederherstellung der Infrastruktur erforderlich sind. Für zeitkritische Entstörungs- und Wiederherstellungsmaßnahmen sollten zudem klare gesetzliche Grundlagen für den Zugang zu erforderlichen

Flächen geschaffen werden, damit Reparaturen, Ersatzbauwerke oder provisorische Maßnahmen im Krisenfall nicht an fehlenden Nutzungs- oder Betretungsrechten scheitern. Dabei gewinnen neben dauerhaft installierten Schutzmaßnahmen auch mobile und flexible Schutz- und Wiederherstellungskonzepte zunehmend an Bedeutung.

Die schnelle Wiederherstellung der Stromversorgung setzt nicht nur geeignete Notfallkonzepte voraus, sondern auch funktionierende Rahmenbedingungen außerhalb der eigentlichen Netzinfrastruktur. Hierzu zählen insbesondere Transportmöglichkeiten für Großkomponenten, verfügbare Verkehrswege, Schwerlasttransportkapazitäten sowie die kurzfristige Bereitstellung erforderlicher Genehmigungen. Physische Resilienz endet daher nicht an der Umzäunung einer Anlage, sondern umfasst die gesamte Fähigkeit zur Wiederherstellung kritischer Infrastruktur nach einem Schadensereignis. Die Verfügbarkeit geeigneter Verkehrs- und Transportinfrastrukturen ist damit selbst ein wichtiger Resilienzfaktor.

Die physische Resilienz des Stromnetzes wird darüber hinaus durch vielfältige Abhängigkeiten von anderen kritischen Infrastrukturen beeinflusst. Hierzu zählen insbesondere Telekommunikation, Informationstechnologie, Verkehrsinfrastruktur, Wasserversorgung und Verwaltungsstrukturen. Störungen in diesen Bereichen können unmittelbare Auswirkungen auf den Netzbetrieb und die Wiederherstellungsfähigkeit haben. Physische Resilienz muss deshalb stets sektorenübergreifend gedacht werden.

Die Anpassung an die Auswirkungen des Klimawandels als weiteres Handlungsfeld nimmt an Bedeutung zu. Hierfür bedarf es eines kohärenten, europäischen Rahmens mit einer übergeordneten EU-Strategie und verpflichtenden nationalen Klimaresilienzplänen, die beispielsweise in die National Energy and Climate Plans (NECPs) integriert werden könnten, um einen harmonisierten Ansatz in den Mitgliedstaaten sicherzustellen. Flankierend sind europaweit einheitliche Standards für Klimarisikoanalysen erforderlich. Gleichzeitig müssen Klimaresilienzmaßnahmen von Übertragungsnetzbetreibern regulatorisch vollständig anerkannt werden, damit notwendige Investitionen in Planung, Bau und Betrieb der Netzinfrastruktur nicht zu finanziellen Risiken führen. Die Berücksichtigung von Klimarisiken in Flächennutzungs- und Bebauungsplänen sowie die Risikobewertung bestehender Baugebiete sind wesentliche Elemente einer wirksamen Klimaanpassung. Gleichzeitig muss sichergestellt werden, dass entsprechende Anforderungen die Umsetzung kritischer Infrastrukturvorhaben nicht unverhältnismäßig erschweren. Für den Netzausbau als Voraussetzung für Energiewende, Versorgungssicherheit und Klimaschutz sollte daher ein ausdrücklicher Vorrang im Planungs- und Genehmigungsrecht vorgesehen werden.

Eine besondere Herausforderung stellen unbemannte Luftfahrzeuge dar. Drohnen stellen für kritische Infrastrukturen eine wachsende Bedrohung dar. Sie können zur Aufklärung sensibler Anlagen, zur Vorbereitung von Sabotagehandlungen oder als unmittelbares Angriffsmittel eingesetzt werden. Gleichzeitig entwickeln sich Technologien und Einsatzmöglichkeiten sehr dynamisch, wodurch neue Verwundbarkeiten entstehen. Für Betreiber kritischer Infrastrukturen ergeben sich hieraus neue Anforderungen an Lageerkennung und Risikoüberwachung.

Aus Sicht der Übertragungsnetzbetreiber bedarf es daher klarer Zuständigkeiten, eindeutiger Rechtsgrundlagen und einer engen Einbindung der Betreiber in bestehende Lagebilder und Sicherheitsstrukturen. Ziel sollte dabei nicht die Übertragung hoheitlicher Gefahrenabwehr auf Betreiber sein. Entscheidend ist vielmehr die rechtssichere Ermöglichung eigener Lageerkennung und Detektion, damit Sicherheitsbehörden frühzeitig informiert, Risiken schneller bewertet und Reaktionszeiten verkürzt werden können. Dies betrifft insbesondere den Einsatz von Videoüberwachung und anderen Detektionssystemen, bei denen datenschutzrechtliche Anforderungen den besonderen Schutzbedürfnissen kritischer Infrastrukturen angemessen Rechnung tragen sollten. Gleichzeitig sollten Zuständigkeiten, Unterstützungsleistungen und Reaktionsprozesse staatlicher Stellen bei Drohnenvorfällen eindeutig definiert werden. Die Zusammenarbeit mit Polizei, Sicherheitsbehörden und dem Gemeinsamen Drohnenabwehrzentrum sollte weiter ausgebaut werden, um Informationen frühzeitig auszutauschen und abgestimmte Reaktionsmechanismen zu etablieren.

Gerade bei hybriden Bedrohungen zeigt sich die Bedeutung einer klaren Rollenverteilung zwischen Staat und Betreibern. Betreiber können Risiken erkennen, Schutzmaßnahmen umsetzen und die Resilienz ihrer

Infrastruktur stärken. Aufgaben der Gefahrenabwehr und Intervention verbleiben jedoch grundsätzlich beim Staat. Physische Resilienz kritischer Energieinfrastrukturen erfordert daher eine enge Verzahnung von Betreibern und staatlichen Stellen bei Lagefeststellung, Prävention, Krisenreaktion und Wiederherstellung.

Dies gilt insbesondere in großflächigen Krisenlagen sowie im Spannungs-, Verteidigungs- oder Bündnisfall. Auch unter außergewöhnlichen Rahmenbedingungen muss sichergestellt werden, dass Betreiber kritischer Infrastrukturen ihre Anlagen erreichen, instandsetzen und betreiben können. Die Aufrechterhaltung dieser Handlungsfähigkeit ist eine wesentliche Voraussetzung für die Funktionsfähigkeit des Energiesystems und damit für die Versorgungssicherheit insgesamt.

3.2 Materialverfügbarkeit und Lieferketten

Die Resilienz kritischer Energieinfrastrukturen hängt maßgeblich von der Verfügbarkeit von Materialien, Komponenten sowie Montage-, Bau-, Wartungs- und Ingenieurleistungen ab. Eine leistungsfähige und resiliente Lieferkette ist Voraussetzung dafür, dass Netzausbau, Instandhaltung, Entstörung und Wiederherstellung auch unter erschwerten Bedingungen zuverlässig gewährleistet werden können. Resilienz beginnt dabei nicht erst im Krisenfall, sondern bereits bei einer vorausschauenden Planung von Bedarfen, Kapazitäten und Beschaffungsprozessen.

Planbarkeit bildet die Grundlage für eine hohe Materialverfügbarkeit. Während Resilienz die Handlungsfähigkeit in unerwarteten Krisenlagen stärkt, ermöglicht eine verlässliche Bedarfsplanung die frühzeitige Vermeidung von Engpässen. Insbesondere bei Komponenten mit langen Produktions- und Lieferzeiten sind belastbare Forecasts von zentraler Bedeutung, um Herstellern und Dienstleistern die rechtzeitige Planung von Produktions-, Personal- und Montagekapazitäten zu ermöglichen. Dies betrifft sowohl materielle Warengruppen wie Transformatoren, Schaltanlagen, Leiterseile, Kabel, Isolatoren oder Notstromaggregate als auch Dienstleistungen wie Montagekapazitäten, Ingenieurleistungen und Bauleistungen. Eine resiliente Lieferkette erfordert deshalb eine enge Zusammenarbeit zwischen Netzbetreibern, Herstellern und Dienstleistern entlang der gesamten Wertschöpfungskette.

Neben der Planbarkeit kommt der Standardisierung eine wichtige Rolle zu. Einheitliche Anforderungen, Spezifikationen und Qualifizierungsprozesse können dazu beitragen, Beschaffungsprozesse zu vereinfachen, die Austauschbarkeit von Komponenten zu erhöhen und die Verfügbarkeit von Lieferanten zu verbessern. Standardisierung erhöht damit nicht nur die Effizienz, sondern stärkt zugleich die Resilienz von Lieferketten und Wiederherstellungsprozessen.

Die zunehmenden geopolitischen Spannungen rücken darüber hinaus strategische Abhängigkeiten in den Fokus. Kritische Energieinfrastrukturen sind auf eine Vielzahl spezialisierter Komponenten angewiesen, deren Herstellung teilweise auf wenige Anbieter oder einzelne Staaten konzentriert ist. Dies betrifft insbesondere Transformatoren, Schaltanlagen, Leistungselektronik und weitere Schlüsselkomponenten mit langen Beschaffungs- und Produktionszeiten. Vor diesem Hintergrund sollte geprüft werden, wie Abhängigkeiten von Drittstaaten reduziert und die Versorgungssicherheit bei kritischen Komponenten gestärkt werden können. Dabei stellt sich insbesondere die Frage, welche Anforderungen künftig an Herkunft, Betrieb, Wartung und Weiterentwicklung sicherheitsrelevanter Komponenten gestellt werden sollten und wie mit veränderten geopolitischen Rahmenbedingungen während der langen Lebensdauer solcher Betriebsmittel umzugehen ist.

Resiliente Lieferketten setzen nicht nur eine sichere Beschaffung voraus, sondern auch ausreichende Produktions-, Wartungs- und Reparaturkapazitäten. Die Verfügbarkeit kritischer Komponenten hängt langfristig davon ab, dass entsprechende industrielle Fähigkeiten erhalten und weiterentwickelt werden. Aus Resiliensicht sollten daher nicht nur Lieferketten, sondern auch Produktions- und Instandsetzungskapazitäten für kritische Betriebsmittel stärker in den Blick genommen werden. Engpässe bei Montage-, Bau- und Instandsetzungskapazitäten können die Wiederherstellungsdauer im Störungs- oder Krisenfall ebenso stark beeinflussen wie fehlende Ersatzteile.

Gleichzeitig erfordern Resilienz und Wiederherstellungsfähigkeit eine bewusste Abwägung zwischen Effizienz und Verfügbarkeit. Die Lagerhaltung von Ersatzteilen, Materialreserven und kritischen Komponenten bindet Kapital und verursacht laufende Kosten. Ihr Nutzen zeigt sich häufig erst im Krisen- oder Schadensfall. Angesichts veränderter Bedrohungslagen gewinnt die strategische Bevorratung ausgewählter Betriebsmittel jedoch zunehmend an Bedeutung. Umfang und Ausgestaltung entsprechender Reserven sollten sich an der Kritikalität der Komponenten, den Wiederbeschaffungszeiten sowie den möglichen Auswirkungen eines Ausfalls orientieren.

Dabei können sowohl unternehmensindividuelle Vorratskonzepte als auch gemeinsame Reserve- und Unterstützungskonzepte einen Beitrag zur Resilienz leisten. Angesichts zunehmender geopolitischer Risiken und langer Wiederbeschaffungszeiten sollte darüber hinaus geprüft werden, ob für besonders kritische Betriebsmittel gemeinsame nationale oder europäische Reservekonzepte sinnvoll und praktikabel sein können. Voraussetzung hierfür sind geeignete organisatorische Strukturen, eine ausreichende technische Kompatibilität der betroffenen Komponenten sowie klare Regelungen für Zugriff, Finanzierung und Einsatz im Krisenfall. Entscheidend ist dabei, dass kritische Betriebsmittel und Dienstleistungen im Bedarfsfall tatsächlich verfügbar sind und die Wiederherstellung der Infrastruktur nicht an fehlenden Komponenten, Transportkapazitäten, Montageleistungen oder Spezialdienstleistern scheitert. Die regulatorischen Rahmenbedingungen sollten dieser Bedeutung Rechnung tragen und den Aufbau resilienzrelevanter Lager- und Reservekonzepte ermöglichen.

Schließlich sollte darauf geachtet werden, dass regulatorische Anforderungen die Resilienz von Lieferketten stärken und nicht unbeabsichtigt schwächen. Angesichts bereits bestehender Engpässe und langer Lieferzeiten sollten zusätzliche Vorgaben sorgfältig auf ihre Auswirkungen auf Verfügbarkeit, Kosten und Realisierungszeiten geprüft werden. Dies gilt insbesondere für sektorspezifische Beschaffungsvorgaben, die für öffentliche Unternehmen den Marktzugang zu Netzkomponenten oder für den Netzausbau notwendige Baumaterialien einschränken können. Vor diesem Hintergrund sollten Stromnetze und die hierfür erforderlichen Technologien von entsprechenden Anforderungen, wie sie im Rahmen des Industrial Accelerator Act auf EU-Ebene diskutiert werden, ausgenommen werden, um den rechtzeitigen Aus- und Umbau der Energieinfrastruktur nicht zu gefährden. Ziel muss es sein, Versorgungssicherheit, Resilienz und Wettbewerbsfähigkeit gleichermaßen zu stärken, ohne die Beschaffung kritischer Komponenten unnötig zu erschweren. Priorität sollten angebotsseitige Maßnahmen und Investitionsanreize haben, die den Ausbau der europäischen Produktionsbasis fördern und einen verlässlichen Zugang zu hochwertigen, wettbewerbsfähigen und resilienten Netztechnologien aus europäischer Fertigung gewährleisten.

3.3 Technologie und System- und digitale Resilienz

Die Digitalisierung des Energiesystems eröffnet neue Möglichkeiten für einen sicheren, effizienten und flexiblen Netzbetrieb. Gleichzeitig entstehen neue Abhängigkeiten und Verwundbarkeiten. Die Resilienz kritischer Energieinfrastrukturen hängt heute nicht mehr allein von physischen Anlagen und Betriebsmitteln ab, sondern zunehmend auch von digitalen Komponenten, Kommunikationssystemen, Softwareplattformen und datenbasierten Prozessen. Technologie- und Systemresilienz bedeutet daher, technologische Innovationen und die fortschreitende Digitalisierung so zu gestalten, dass Versorgungssicherheit und Systemstabilität dauerhaft gewährleistet bleiben.

Mit dem Wandel des Energiesystems steigt die Anzahl neuer Marktteilnehmer und technischer Komponenten mit unmittelbarer Relevanz für den sicheren Netzbetrieb. Batteriespeicher, Wechselrichter, Elektrolyseure, Aggregatoren und weitere digital gesteuerte Anlagen übernehmen zunehmend systemrelevante Funktionen. Gleichzeitig verfügen Übertragungsnetzbetreiber vielfach nur über begrenzte Einblicke in die technischen Eigenschaften, Kommunikationsstrukturen und Sicherheitsmechanismen dieser Systeme. Aus Resilienz-sicht ist daher sicherzustellen, dass für alle systemrelevanten Komponenten ein angemessenes Sicherheitsniveau sowie einheitliche technische Mindeststandards gelten. Resilienz-anforderungen sollten dabei von Beginn an berücksichtigt werden und nicht erst nachträglich entstehen.

Mit dem Umbau des Energiesystems gewinnen darüber hinaus die Steuerbarkeit und Beobachtbarkeit dezentraler Erzeugungs- und Speicheranlagen zunehmend an Bedeutung. Fähigkeiten, die bislang überwiegend von

konventionellen Kraftwerken erbracht wurden, müssen künftig in einem deutlich dezentraleren Energiesystem gewährleistet werden. Die sichere Steuerung von Leistungsflüssen ist dabei eine wesentliche Voraussetzung für die Resilienz und Stabilität des Stromsystems. Voraussetzung hierfür sind die konsequente Umsetzung bestehender Anforderungen an die Steuerbarkeit von Erzeugungs- und Speicheranlagen, ein beschleunigter Rollout intelligenter Messsysteme sowie eine klare Zuordnung von Verantwortlichkeiten zwischen Messstellenbetreibern, Netzbetreibern und weiteren Marktakteuren. Die zunehmende Digitalisierung des Energiesystems darf nicht zu neuen Intransparenzen oder Steuerungslücken führen, sondern muss die Handlungsfähigkeit der Netzbetreiber stärken.

Besondere Bedeutung kommt der zunehmenden Vernetzung digitaler und physischer Infrastrukturen zu. Kommunikationssysteme, Fernwirktechnik, Sensorik, Softwareplattformen und automatisierte Steuerungsfunktionen werden für den Netzbetrieb immer wichtiger. Ausfälle, Fehlfunktionen oder Manipulationen digitaler Komponenten können dadurch unmittelbare Auswirkungen auf die Stabilität des Energiesystems haben. Die Auswirkungen neuer Technologien auf die Systemsicherheit sollten daher frühzeitig bewertet und bei regulatorischen sowie technischen Entscheidungen berücksichtigt werden.

Ein weiteres Handlungsfeld ergibt sich aus der zunehmenden Bedeutung zentraler Plattformen und digitaler Steuerungsstrukturen. Hersteller, Dienstleister und Plattformbetreiber erhalten teilweise weitreichende technische Zugriffsmöglichkeiten auf Komponenten des Energiesystems. Daraus entstehen neue Abhängigkeiten und potenzielle Risiken für die Versorgungssicherheit. Für systemrelevante Anlagen sollte daher jederzeit sichergestellt sein, dass Zuständigkeiten, Zugriffsmöglichkeiten und Sicherheitsanforderungen klar geregelt sind und die für die Systemsicherheit erforderliche Steuerbarkeit dauerhaft gewährleistet bleibt. Übertragungsnetzbetreiber müssen in der Lage bleiben, ihre Systemverantwortung auch in einem zunehmend dezentralen und digitalisierten Energiesystem wirksam wahrzunehmen.

Technologische Resilienz umfasst darüber hinaus die Frage der digitalen Souveränität. Kritische Energieinfrastrukturen sind zunehmend von Hard- und Softwarekomponenten, Cloud-Diensten und digitalen Plattformen abhängig, die teilweise außerhalb Europas entwickelt, betrieben oder kontrolliert werden. Vor dem Hintergrund geopolitischer Spannungen und wachsender Sicherheitsanforderungen sollte geprüft werden, wie digitale Abhängigkeiten reduziert und europäische Kompetenzen in strategisch wichtigen Technologiefeldern gestärkt werden können. Dies betrifft insbesondere sicherheitsrelevante Technologien, digitale Plattformen, Kommunikationslösungen und Cloud-Infrastrukturen, die für den Betrieb kritischer Infrastrukturen von zentraler Bedeutung sind.

Da das Stromsystem Teil eines europäischen Verbundnetzes ist, sollten Resilienzanforderungen möglichst kohärent und grenzüberschreitend betrachtet werden. Technische Standards, Sicherheitsanforderungen und regulatorische Vorgaben sollten auf europäischer Ebene möglichst konsistent ausgestaltet werden, um Fragmentierungen, Doppelregulierungen und neue Verwundbarkeiten zu vermeiden. Gleichzeitig können gemeinsame europäische Standards, abgestimmte Sicherheitsanforderungen sowie der Aufbau eigener europäischer Technologiekompetenzen und digitaler Infrastrukturen dazu beitragen, die Resilienz des Energiesystems insgesamt zu stärken. Die Stärkung europäischer Technologiekompetenzen und digitaler Souveränität ist damit nicht nur ein industriepolitisches Ziel, sondern zunehmend auch eine Frage der Versorgungssicherheit und Resilienz kritischer Infrastrukturen.

4. Personelle Resilienz

Resilienz erfordert darüber hinaus die Stärkung der personellen Sicherheit als integralen Bestandteil kritischer Infrastrukturen. Sicherheitsüberprüfungen für Mitarbeitende in sensiblen Funktionen leisten hierzu einen wichtigen Beitrag. Die datenschutzrechtlichen Rahmenbedingungen sollten dabei so ausgestaltet werden, dass wirksame und verhältnismäßige Sicherheitsprüfungen unbürokratisch durchgeführt werden können. Insbesondere bei behördenübergreifenden Prüf- und Informationsprozessen bestehen Potenziale für eine stärkere Digitalisierung sowie einen Ausbau personeller Ressourcen auf Behördenseite. Dies würde dazu beitragen, Verfahren zu beschleunigen und die zeitnahe Besetzung sicherheitsrelevanter Positionen im KRITIS-Sektor zu erleichtern. Gleichzeitig ist die Sicherung ausreichender Fachkräftekapazitäten eine wesentliche Voraussetzung für die Resilienz kritischer Infrastrukturen. Angesichts des zunehmenden Fachkräftemangels sollten Ausbildung, Qualifizierung und Gewinnung von Fachpersonal in KRITIS-relevanten Berufen gezielt unterstützt werden.

Ihre Ansprechpartner

Florian Reuter

Teamleiter
Nationale Energiepolitik

f.reuter@transnetbw.de

Dr.-Ing. Michael Heihsel

Hauptstadtrepräsentant
Nationale Energiepolitik

m.heihsel@transnetbw.de

Vanessa Bausch

Spezialistin
European Affairs

v.bausch@transnetbw.de