amprion
verbindet

LEITPLANKEN FÜR EINE RESILIENTE STROMINFRASTRUKTUR

ZENTRALE HANDLUNGSFELDER UND EMPFEHLUNGEN FÜR GESETZLICHE ANPASSUNGEN

JUNI 2026

VORWORT

Die Sicherheitslage in Europa hat sich mit dem Angriff der Russischen Föderation auf die Ukraine seit Anfang 2022 deutlich verschärft: Deutschland und die Europäische Union sind zunehmend hybriden Bedrohungen ausgesetzt, die gezielt gegen Kritische Infrastrukturen (KRITIS) gerichtet sind. Dazu zählen Ausspähversuche wie nahezu tägliche Überflüge von unbekannten Drohnen über Anlagen der Kritischen Infrastruktur, Cyberangriffe und physische Angriffe. Neben Sabotageversuchen dienen diese Aktivitäten auch als Reaktionstests, um für spätere Angriffe Schlupflöcher in den Sicherheitssystemen zu finden.

Zugleich nimmt Kriminalität im digitalen wie im physischen Raum zu und zielt immer häufiger auf Anlagen und Systeme des Netzbetriebs – dazu zählen Einbrüche auf Baustellen und Umspannanlagen zum Diebstahl wertvoller Materialien genauso wie digitale Betrugs- und Erpressungsfälle. Hinzu kommen politisch motivierte terroristische Anschläge, die darauf abzielen, besonders vulnerable Stellen des Stromsystems zu treffen und dieses zu destabilisieren. Der Anfang Januar 2026 durch einen Brandanschlag verursachte Stromausfall im Südwesten Berlins, der in Teilen bis zu fünf Tage andauerte und zu dem sich Täter aus dem linksextremen Spektrum bekannt haben, hat eindrücklich gezeigt, welche gesellschaftlichen Verwerfungen bereits eine lokal begrenzte Versorgungsunterbrechung nach sich zieht.

Parallel dazu verschärft auch der Klimawandel die Rahmenbedingungen für einen sicheren Netzbetrieb. Extremwetterereignisse und Naturkatastrophen wie die Ahrtal-Flutkatastrophe im Jahr 2021, das Donauhochwasser in Baden-Württemberg und Bayern im Jahr 2024 oder der Tornado in Sachsen im Jahr 2025, der mehrere Strommasten zerstörte, treffen zunehmend die KRITIS.

Der Standort Deutschland, die hier lebenden Menschen und unsere Wirtschaft sind auf eine sichere Stromversorgung angewiesen. Ein eng vermaschtes, europaweites Stromnetz kann jedoch nicht an jedem Punkt lückenlos geschützt werden – allein Amprion betreibt über 200 Umspannanlagen, mehr als 11.000 Kilometer Leitungen und eine Vielzahl an IT-Systemen. Umso wichtiger sind Vorsorge, Reaktionsfähigkeit und die schnelle Wiederherstellung des Normalbetriebs, wenn es zu einer Störung gekommen ist.

Amprion bereitet sich seit vielen Jahren auf Störungsszenarien vor, passt interne Prozesse kontinuierlich an die Bedrohungslage an und übt regelmäßig Krisenabläufe. Unabhängig davon ist klar: Resilienz ist eine gesamtgesellschaftliche Aufgabe. Sie erfordert verlässliche rechtliche Rahmenbedingungen, klare Zuständigkeiten, eine enge Zusammenarbeit zwischen Behörden und KRITIS-Unternehmen sowie eine angemessene Finanzierung von Maßnahmen zur Steigerung der Resilienz. Bei allen derzeitigen Debatten gilt es zugleich festzuhalten: Die hoheitliche Aufgabe der Gefahrenabwehr liegt in der Hand der Sicherheitsbehörden.

Dieses Positionspapier beschreibt aus der Sicht von Amprion wichtige Handlungsfelder und konkrete Vorschläge für die Weiterentwicklung des regulatorischen Rahmens, um das Stromnetz für die Herausforderungen der Zukunft sicher aufzustellen.

DR. CHRISTOPH MÜLLER
Chief Executive Officer (CEO)

DR. HENDRIK NEUMANN
Chief Technical Officer (CTO)

ZUSAMMENFASSUNG DER ZENTRALEN FORDERUNGEN

RECHTSRAHMEN UND VERWALTUNGSPRAXIS FÜR KRITIS KRISENFEST GESTALTEN

1. **Rechtsrahmen für KRITIS-Betreiber an aktuelle Sicherheitslage anpassen**
Übertragungsnetzbetreiber brauchen eine rechtliche Sonderstellung, die ihnen in Krisen schnelle, unbürokratische Handlungsspielräume eröffnet, um die Stromversorgung zu sichern oder wiederherzustellen. Dafür sind konsistente und praxisnahe gesetzliche Regelungen erforderlich, die bundesländer- und rechtsgruppenübergreifend harmonisiert sein sollten.

2. **Veröffentlichungs- und Transparenzpflichten reduzieren und Zugang zu KRITIS-Informationen beschränken**
Die umfassenden Transparenz- und Veröffentlichungspflichten müssen so angepasst werden, dass sicherheitsrelevante KRITIS-Informationen systematisch geschützt, der Detailgrad veröffentlichter Netzdaten reduziert und der Zugriff auf berechtigte Nutzer beschränkt wird. Dafür sind unter anderem Ausnahmen im Energie-, Umweltinformations- und Vergaberecht sowie eine Reform der Offenlegungspflichten im Lobbyregistergesetz nötig.

3. **Öffentlichkeitsbeteiligung auf das notwendige Maß begrenzen**
Die Öffentlichkeitsbeteiligung in Planungs- und Genehmigungsverfahren muss so ausgestaltet werden, dass nur die notwendigen Informationen offengelegt werden und sicherheitsrelevante Details zu KRITIS-Anlagen geschützt bleiben. Dafür braucht es eine geringere Detailtiefe der veröffentlichten Unterlagen, einen gesteuerten Zugang (zum Beispiel Need-to-know-Logik und begrenzte Zugriffsberechtigungen nach dem Berechtigtenprinzip) sowie Möglichkeiten zur Einschränkung der Öffentlichkeit in Gerichtsverfahren.

4. **Notfall- und Entstörungsmaßnahmen unbürokratisch ermöglichen**
Notfall- und Entstörungsmaßnahmen müssen für Übertragungsnetzbetreiber rechtssicher und unbürokratisch möglich sein, damit Leitungen und Anlagen im Krisenfall schnell erreicht, repariert und provisorisch wiederhergestellt werden können. Dazu braucht es klare Betretungsrechte, erleichterte bzw. gebündelte Genehmigungen, priorisierte Schwerlasttransporte sowie abgestimmte Katastrophenschutzpläne und – perspektivisch – eine strategische Notreserve kritischer Betriebsmittel.

ZUSAMMENFASSUNG DER ZENTRALEN FORDERUNGEN

SCHUTZ, ÜBERWACHUNG UND DATENVERARBEITUNG ANLAGENBEZOGEN STÄRKEN

5. **Überwachung der eigenen Anlagen pragmatisch ermöglichen**
KRITIS-Betreiber müssen ihre Anlagen mit Mitteln wie BVLOS-Drohnenflügen, Videoüberwachung und Drohnendetektion flächendeckend und rechtskonform überwachen können, ohne durch unverhältnismäßige Genehmigungs- und Datenschutzvorgaben ausgebremst zu werden. Ziel ist eine deutlich verbesserte Lageerkennung zur schnellen Einschaltung der Sicherheitsbehörden.

6. **Klaren Rechtsrahmen für Datenverarbeitung und Datenschutz schaffen**
Die Überwachung der eigenen Anlagen ist nur dann möglich, wenn es eine klare Rechtsgrundlage für die Verarbeitung und Speicherung personenbezogener Daten bei den Übertragungsnetzbetreibern gibt.

7. **Objektschutz und Anlagenhärtung von Genehmigungspflicht befreien**
Objektschutz- und Härtungsmaßnahmen müssen schnell und ohne unnötige bürokratische Hürden umgesetzt werden können. Dafür braucht es die umfassende Befreiung von der Baugenehmigungspflicht für Nebenanlagen wie Zäune und Torsysteme (über die Landesbauordnungen) sowie vereinfachte Genehmigungen beim Austausch von Transformatoren.

INFRASTRUKTUR UND NETZPLANUNG RESILIENT UND FINANZIERUNGSSICHER GESTALTEN

8. **Verkehrsinfrastruktur als Voraussetzung für Resilienz stärken**
Die Resilienz des Stromnetzes hängt unmittelbar von einer leistungsfähigen Verkehrsinfrastruktur ab, die Schwerlasttransporte kritischer Betriebsmittel schnell und flexibel ermöglicht. In der Verkehrsplanung und bei der Instandhaltung der Verkehrswege müssen deshalb die Anforderungen des Stromnetzes berücksichtigt werden.

9. **Resilienzorientierte Netzplanung ermöglichen**
Die Netzplanung muss Resilienz als eigenständiges Ziel neben der volkswirtschaftlichen Effizienz anerkennen und Geo-Redundanz für besonders kritische Netzelemente ermöglichen. Dazu braucht es einen Resilienzfaktor im Netzentwicklungsplan und erweiterte Möglichkeiten für die Planung von Leistungsreserven.

10. **Kritische Infrastruktur bei konkurrierenden Vorhaben priorisieren**
Netzausbau- und Stationsvorhaben der Übertragungsnetzbetreiber sollten bei konkurrierenden Projekten im überragenden öffentlichen Interesse gesetzlich als besonders gewichtiger Abwägungsbelang priorisiert werden.

ZUSAMMENFASSUNG DER ZENTRALEN FORDERUNGEN

11. **Finanzierbarkeit, Kostenanerkennung und Lieferketten für kritische Komponenten sichern**
Resilienzmaßnahmen im Stromnetz verursachen erhebliche Mehrkosten und dürfen weder die Investitionsfähigkeit der Übertragungsnetzbetreiber einschränken noch regulatorisch als Ineffizienzen bestraft werden. Deshalb braucht es eine vollständige, zügige Kostenanerkennung der Investitionen in Resilienz, des betrieblichen Mehraufwands und einer dezentralen Lagerhaltung. Lieferketten für kritische Betriebsmittel wie Transformatoren sollten durch einen politisch unterstützten Branchendialog gesichert werden.

KOOPERATION, ZUGRIFFSRECHTE UND INFORMATIONSAUSTAUSCH AUSBAUEN

12. **Krisenprävention: Austausch und Übungen mit Sicherheitsbehörden intensivieren**
Um in Krisensituationen handlungsfähig zu bleiben, müssen Sicherheitsbehörden und Netzbetreiber ihre Lagebilder miteinander teilen, Notfallpläne abstimmen und gemeinsam üben und schwarzfallfeste Kommunikationswege etablieren. Bei Störungen braucht es polizeiliche Begleitung und Zugangsregelungen, damit das Betriebspersonal der Netzbetreiber schnell mit Entstörungsarbeiten beginnen kann.

13. **Zugriffsrechte der Übertragungsnetzbetreiber auf Daten und Netzelemente sicherstellen**
Die Übertragungsnetzbetreiber benötigen in einem zunehmend dezentralen Energiesystem verlässliche Zugriffsrechte auf Steuerungsfunktionen und netzrelevante Daten, um ihre Systemverantwortung wahrnehmen zu können. Dafür müssen die gesetzlich geforderte Steuerbarkeit dezentraler Anlagen konsequent durchgesetzt sowie Betreiberpflichten und Sicherheitsstandards für Herstellerplattformen EU-weit geregelt werden.

14. **Die europäische Dimension der Resilienz stärken**
Die Resilienz des europäischen Stromsystems muss als gemeinschaftliche Aufgabe verstanden werden, bei der Transparenz-, Sicherheits- und Resilienzvorgaben EU-weit aufeinander abgestimmt und Doppelregulierungen vermieden werden. Dazu braucht es aktualisierte, zügig verabschiedete technische Regeln (zum Beispiel Network Codes) sowie die gemeinsame Förderung von Fachkräften und europäischer Sicherheits- und Cloudtechnologien.

GRUNDLAGEN DER RESILIENZ – VERSTÄNDNIS UND DIMENSIONEN

Die Resilienz der Strominfrastruktur bedeutet mehr als reine technische Versorgungssicherheit. Amprion verfolgt einen All-Gefahren-Ansatz und stärkt Resilienz auf Basis eines systematischen Risikomanagements. Neben der physischen Resilienz und der Sicherung des gesetzlichen Versorgungsauftrags stehen für Amprion daher auch die Informationssicherheit und die personelle Sicherheit im Fokus. Aus der Sicht von Amprion umfasst Resilienz drei Dimensionen, in denen ein Stromnetzbetreiber handlungsfähig sein muss, um seinen gesetzlichen Versorgungsauftrag zu erfüllen:

1. **WIDERSTANDSFÄHIGKEIT/SCHUTZ UND ROBUSTHEIT**
   DIE FÄHIGKEIT DER ANLAGEN, LEITUNGEN, BETRIEBSMITTEL, OT- UND IT-KOMMUNIKATIONSSYSTEME SOWIE ORGANISATION UND MITARBEITENDEN, EXTERNEN UND INTERNEN EINFLÜSSEN WIE PHYSISCHEN UND DIGITALEN ANGRIFFEN ODER EXTREMWETTEREREIGNISSEN STANDZUHALTEN UND DEN STABILEN NETZBETRIEB AUFRECHTZUERHALTEN.

2. **ANPASSUNGSFÄHIGKEIT**
   DIE FÄHIGKEIT, IM STÖRUNGSFALL SCHNELL, KOORDINIERT UND WIRKSAM ZU HANDELN, UM LÄNGERFRISTIGE SCHÄDEN AN BETRIEBSMITTELN UND VERSORGUNGSUNTERBRECHUNGEN ZU VERHINDERN. DER NETZBETREIBER BEHÄLT DIE KONTROLLE UND BLEIBT HANDLUNGSFÄHIG.

3. **WIEDERHERSTELLUNGSFÄHIGKEIT**
   DIE ZEITNAHE RÜCKKEHR VON EINEM STÖRUNGSEREIGNIS IN EINEN STABILEN NORMALBETRIEB UND IN LETZTER KONSEQUENZ AUCH DIE SCHNELLE WIEDERHERSTELLUNG DER STROMVERSORGUNG.

Ein kontinuierliches Lagebild, klare Krisen- und Entscheidungsstrukturen sowie regelmäßige Risikoanalysen, Übungen und Reviews unterstützen hierbei und gewährleisten Handlungsfähigkeit. Resilienz wird bei Amprion als integraler Bestandteil aller Geschäfts- und Betriebsprozesse verstanden – eine zentrale Grundlage dafür, die besondere Verantwortung als KRITIS-Betreiber dauerhaft und verlässlich wahrzunehmen.

Neben der Kenntnis der eigenen Risikoexposition und der zielgenauen Vorbereitung auf diese Risiken ist das regulatorische Umfeld bedeutsam, da es den Handlungsspielraum des Unternehmens vor und besonders in Krisenlagen definiert.

Die gesetzlichen Grundlagen im Umfeld der Resilienz Kritischer Infrastrukturen sind vielfältig (unter anderem Energiewirtschaftsgesetz, KRITIS-Dachgesetz, NIS-2-Richtlinie, BSI-Gesetz, Luftsicherheitsgesetz, Energiesicherungsgesetz, Wirtschaftssicherstellungsgesetz, Katastrophenschutzgesetze der Länder, Konzeption Zivile Verteidigung) und betreffen viele unterschiedliche Zuständigkeitsbereiche. Sie sind derzeit zudem weder konsistent auf die besonderen Anforderungen von KRITIS-Betreibern zugeschnitten noch hinreichend genau auf die verschärfte Sicherheitslage ausgerichtet. Amprion sieht die Notwendigkeit normativer Anpassungsbedarfe, um den Anforderungen an ein resilientes Stromnetz auch in Zukunft erfolgreich begegnen zu können.

Die folgenden Handlungsfelder zeigen aus der Sicht von Amprion auf, in welchen Bereichen gesetzliche Anpassungen und vertiefte Zusammenarbeit dringend erforderlich sind, um diese Aufgabe erfüllen zu können.

HANDLUNGSFELDER FÜR EINE RESILIENTE STROMINFRASTRUKTUR

RECHTSRAHMEN UND VERWALTUNGSPRAXIS FÜR KRITIS KRISENFEST GESTALTEN

1 RECHTSRAHMEN FÜR KRITIS-BETREIBER AN AKTUELLE SICHERHEITSLAGE ANPASSEN

AUSGANGSLAGE

Übertragungsnetzbetreiber tragen eine besondere Verantwortung für die Stromversorgung und unterliegen durch die besondere regulatorische Stellung bereits heute einer Vielzahl einzelgesetzlicher Anforderungen. Gleichzeitig werden sie rechtlich vielfach wie andere privatwirtschaftliche Unternehmen behandelt. Die bestehenden Regelungen bilden die spezifische Rolle von KRITIS-Betreibern in einer angespannten Sicherheitslage nur unzureichend ab. In Krisen- und Katastrophensituationen erschweren komplexe Verfahren, föderale Bruchlinien und uneinheitliche Zuständigkeiten schnelles, unbürokratisches Handeln.

FORDERUNGEN

Spezifische Rechtsstellung von KRITIS-Betreibern verankern

KRITIS-Betreiber sollten rechtlich ausdrücklich als Akteure mit besonderem Versorgungsauftrag identifiziert werden. Daraus müssen sich neben Pflichten auch besondere Rechte ergeben, die ihrer speziellen Verantwortung Rechnung tragen – insbesondere in Krisensituationen. Netzbetreiber benötigen wirksame Handlungsspielräume, um die Stromversorgung unter widrigen Umständen zu sichern und ggf. wiederherzustellen. In Notsituationen sollte dies auch die Freistellung von Genehmigungspflichten umfassen.

Länderübergreifende Harmonisierung sicherstellen

Das Stromnetz ist ein länderübergreifendes, europäisches Verbundnetz – gerade diese Ausdehnung und Vermaschung stärken die Versorgungssicherheit. Die Katastrophenschutzgesetze sind in Deutschland jedoch größtenteils den Bundesländern zugeordnet. Um rechtliche Abbruchkanten zu vermeiden, ist eine Harmonisierung der Gesetze auf nationaler Ebene anzustreben.

KRITIS-Perspektive in Verordnungen zum KRITIS-Dachgesetz berücksichtigen

Die noch zu erlassenden Rechtsverordnungen zur Umsetzung des KRITIS-Dachgesetzes sollten Mindestanforderungen an die Resilienz Kritischer Infrastrukturen klar benennen und zügig erarbeitet werden. Es ist essenziell, dass die Verordnungen die Bedürfnisse der betroffenen Unternehmen berücksichtigen. Bei der Ausgestaltung der Anforderungen aus dem Umfeld des KRITIS-Dachgesetzes ist zudem zu berücksichtigen, dass diese konsistent zu den Anforderungen aus benachbarten Gesetzesfamilien sind – beispielsweise zur NIS-2-Richtlinie und ihrer nationalen Umsetzung.

2 VERÖFFENTLICHUNGS- UND TRANSPARENZPFLICHTEN REDUZIEREN UND ZUGANG ZU KRITIS-INFORMATIONEN BESCHRÄNKEN

AUSGANGSLAGE

In den vergangenen Jahren haben Transparenz- und Veröffentlichungspflichten, denen Netzbetreiber unterliegen, deutlich zugenommen. Der aktuelle Rechtsrahmen (unter anderem Energiewirtschaftsgesetz (EnWG), Umweltinformationsgesetz (UIG), Informationsfreiheitsgesetz (IFG), Geodatenzugangsgesetz (GeoZG), Gesetz gegen Wettbewerbsbeschränkungen (GWB), Vergabeverordnung (VgV), Sektorenverordnung (SektVO)) wirkt dem Schutzbedarf der Kritischen Infrastruktur teilweise aktiv entgegen, da sensible Informationen öffentlich zugänglich gemacht oder auf Anfrage herausgegeben werden müssen. Die weitere Verwendung dieser Informationen ist nicht kontrollierbar. Nicht zuletzt ermöglichen Daten aus Beschaffungs- und Vergabeverfahren, der Netzentwicklungsplanung und Unterlagen aus Genehmigungsverfahren in ihrer Summe Rückschlüsse auf Netzauslastung, kritische Knotenpunkte und Schwachstellen. Sie erlauben es potenziellen Angreifern, Sabotageziele auszuwählen.

FORDERUNGEN

Transparenzpflichten nach dem EnWG einschränken

Plattformen wie SMARD, das Marktstammdatenregister und die nationale Transparenzplattform (vgl. §§111d-111g EnWG beziehungsweise §15 MaStRV) sowie der Netzentwicklungsplan nach §12b EnWG machen detaillierte Daten zu Netzknoten, Engpässen und Betriebsmitteln öffentlich zugänglich. Das Energiewirtschaftsgesetz erkennt zwar bereits Schutzmöglichkeiten für sensible Daten an, diese Spielräume werden allerdings wegen der Gewichtung der Transparenz bislang nicht genutzt – hier sollten die eingeräumten Möglichkeiten in Abstimmung zwischen Netzbetreibern und Behörden konsequent umgesetzt werden. Zudem sind Detailgrad und Auflösung der Netzdaten systematisch zu reduzieren und stärker zu aggregieren. Der Zugang zu besonders sensiblen Datensätzen sollte zugleich auf Nutzer mit nachgewiesenem berechtigtem Interesse beschränkt werden.

Ausnahmetatbestände ins Umwelt- und Informationsrecht aufnehmen

Die Anwendung von UIG, IFG und GeoZG sollte dahingehend überprüft werden, ob Ablehnungsgründe zum Schutz Kritischer Infrastrukturen gestärkt oder ausgeweitet werden können – beispielsweise durch die Behandlung der Kritischen Infrastruktur als Schutzgut der öffentlichen Sicherheit. Sicherheitsrelevante Informationen könnten dadurch unter einen Veröffentlichungsvorbehalt gestellt und von der Veröffentlichung ausgenommen werden. In einem zentralen Regelwerk – etwa im KRITIS-Dachgesetz beziehungsweise den daran angeschlossenen Umsetzungsverordnungen – könnte dazu eine allgemeine Beschreibung sicherheitsrelevanter Sachverhalte aufgenommen werden, auf die in den einschlägigen Fachgesetzen (insbesondere VwVfG, EnWG, NABEG, BImSchG sowie IFG) ausdrücklich verwiesen werden kann. Denn in der Praxis zeigt sich, dass für Behörden regelmäßig nicht klar ist, nach welchen Kriterien im Einzelfall eine Sicherheitsrelevanz zu begründen ist.

FORDERUNGEN

Staatliche Datenanforderungen auf das Notwendige begrenzen

Behörden sollten nur solche sensiblen Informationen (zum Beispiel Listen kritischer Komponenten nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)) anfordern, die für ihre Aufgabe zwingend erforderlich sind. Gleichzeitig muss der Staat für einen dem Schutzbedarf angemessenen Umgang mit diesen Daten sorgen – etwa durch Nutzung nationaler Infrastruktur, Datenminimierung und die Härtung genutzter Portale.

Vergaberecht auf KRITIS-Belange anpassen

Das Vergaberecht sollte für KRITIS-Betreiber grundsätzlich weiter gelten, aber für sicherheitskritische Beschaffungen angepasst werden. Es braucht die Möglichkeit, vollständige Vergabeunterlagen nur solchen Bietern zur Verfügung zu stellen, deren Eignung bereits vorab geprüft wurde. Für sicherheitskritische Beschaffungen ist zudem ein Ausnahmetatbestand in §13 Abs. 2 SektVO sinnvoll, der ein Verhandlungsverfahren ohne Teilnahmewettbewerb mit beschränktem und geprüftem Bieterkreis zulässt.

Offenlegungspflichten nach dem Lobbyregistergesetz reformieren

In der politischen Interessenvertretung kommunizieren die Übertragungsnetzbetreiber fortlaufend und umfassend mit politischen Entscheidungsträgern im Bundestag und in der Bundesregierung. Der Austausch verfolgt das Ziel, verlässliche und faktenbasierte Entscheidungsgrundlagen zu liefern. Dazu gehören technische Expertise, Systemwissen und praktische Erfahrung in Planung, Bau, Betrieb und Wartung des Netzes. Das Lobbyregistergesetz verpflichtet Unternehmen nach § 3 Abs. 1 Nr. 5 Buchstabe b), Stellungnahmen grundsätzlich zu veröffentlichen, wenn sie der politischen Interessenvertretung dienen. Dies umfasst auch die Kommunikation zu sensiblen Fragestellungen – beispielsweise, wenn Netzbetreiber Anpassungen am regulatorischen Rahmen zum Schutz der Kritischen Infrastrukturvorschlagen und damit auf mögliche Lücken hinweisen. Diese Offenlegungspflichten bedürfen der Reform dahingehend, dass Übertragungsnetzbetreiber nicht mehr vom Lobbyregistergesetz erfasst werden.

Darstellung von KRITIS-Anlagen in Kartendiensten einschränken

Kritische Anlagen- und Lagerstandorte sowie Leitungsverbindungen via Freileitung oder Erdkabel sollten in allgemein zugänglichen Diensten (zum Beispiel Google Maps/Street View) nur eingeschränkt sichtbar oder verpixelt sein. Spezialisierte Tools wie Open Infrastructure Map sollten auf Behörden und Netzbetreiber beschränkt werden können.

3 ÖFFENTLICHKEITSBETEILIGUNG AUF DAS NOTWENDIGE MASS BEGRENZEN

AUSGANGSLAGE

Öffentlichkeitsbeteiligung in Planungs- und Genehmigungsverfahren ist essenziell für die Akzeptanz der Energiewende und auch aus rechtsstaatlicher Sicht zwingend geboten. Die aktuell sehr weitgehenden Offenlegungs- und Beteiligungspflichten führen jedoch dazu, dass sicherheitsrelevante Details zu Anlagen, Leitungsverläufen und Betriebsmitteln in einem Umfang öffentlich werden, der aus Resilienzperspektive problematisch ist. Zugleich sind viele der vom Vorhabenträger zu veröffentlichenden Angaben für die Öffentlichkeit nicht erforderlich, um Betroffenheiten zu beurteilen.

FORDERUNGEN

Detaillierungsgrad in Antragsunterlagen reduzieren

In Infrastrukturverfahren (unter anderem nach Verwaltungsverfahrensgesetz (VwVfG), Energiewirtschaftsgesetz (EnWG), Netzausbaubeschleunigungsgesetz (NABEG), TEN-E-Verordnung, Windenergie-auf-See-Gesetz (WindSeeG), Umweltverträglichkeitsprüfungsgesetz (UVPG), Raumordnungsgesetz (ROG)) sollte der veröffentlichungspflichtige Detaillierungsgrad auf das notwendige Maß beschränkt werden. Allgemeine Beschreibungen und Nachweise über die Einhaltung von Richt- und Grenzwerten sowie weiterer Planungsvorgaben sollten weiterhin öffentlich sein, technische Detailpläne – wie statische Informationen oder Profilpläne von Leitungen – hingegen nur den Trägern öffentlicher Belange (TöB) zur Verfügung stehen.

Geheimschutz stärken

Die Möglichkeiten des Geheimnisschutzes (§ 30 VwVfG) und vergleichbare Instrumente sollten leichter anwendbar und durch Anpassungen der einschlägigen Fachgesetze (insbesondere Bundes-Immissionsschutzgesetz (BImSchG), UVPG, EnWG) rechtssicher auf sicherheitsrelevante Informationen energiewirtschaftlicher Kritischer Infrastruktur ausgedehnt werden.

Teilnehmerkreis bei Erörterungen begrenzen

Bei Erörterungsterminen in Genehmigungsverfahren sollte mit Blick auf sensible Themen eine striktere Begrenzung des Teilnehmerkreises ermöglicht werden, etwa durch Nachweis der Betroffenheit oder getrennte Erörterungen mit beschränktem Zugang für sicherheitsrelevante Aspekte. Insgesamt ist statt einer breiten Veröffentlichung der Need-to-know-Grundsatz denkbar.

Zugang zu sensiblen Unterlagen steuern

Der Einsatz professioneller Datenräume sollte rechtlich abgesichert werden, um Zugriffe zu kontrollieren, Downloads zu beschränken und Unterlagen ggf. nur mit Wasserzeichen zugänglich zu machen. Persönliche Daten können als „Eingangsschranke“ dienen, um nachvollziehbar zu machen, wer welche Informationen abgerufen hat.

Öffentlichkeit in Gerichtsverfahren einschränken können

Für Verfahren, in denen Genehmigungen von KRITIS-Anlagen streitgegenständlich sind, sollte die Möglichkeit geschaffen werden, die Öffentlichkeit auszuschließen, wenn andernfalls sicherheitsrelevante Informationen offengelegt würden. Zu prüfen ist, ob § 172 GVG (i. V. m. § 55 VwGO) hierfür bereits ausreicht oder einer Ergänzung bedarf.

4 NOTFALL- UND ENTSTÖRUNGSMASSNAHMEN UNBÜROKRATISCH ERMÖGLICHEN

AUSGANGSLAGE

Im Ernstfall zählt die Geschwindigkeit: Im Störungs- oder Schadensfall kommt es darauf an, die Stromversorgung so schnell wie möglich zu sichern und gegebenenfalls provisorisch wiederherzustellen. Dafür muss schweres Großgerät wie Transformatoren oder provisorische Strommasten über große Distanzen schnell ans Ziel gebracht und im Nachgang die beschädigte Infrastruktur unverzüglich repariert werden. Heute führt eine Vielzahl beteiligter Rechtsbereiche (Naturschutz-, Immissionsschutz-, Wasser-, Transport-, Eigentums- und Baurecht) zu aufwändigen Genehmigungsverfahren. Für Entstörungsmaßnahmen sind beispielsweise umfassende Einzelgenehmigungen einzuholen – gerade dann, wenn die Zeit drängt und die öffentliche Sicherheit von der zügigen Instandsetzung des Stromnetzes abhängt. Hier braucht es einfache und schnelle Lösungen und pragmatisches Verwaltungshandeln. Das Katastrophenschutzrecht bietet zwar grundsätzlich geeignete Instrumente, ist aber in Bezug auf KRITIS-Anlagen in Teilen unklar oder zu eng gefasst.

FORDERUNGEN

Betretungsrechte für Notfall- und Instandhaltungsarbeiten schaffen

Die Netzbetreiber benötigen für zeitkritische Reparatur- und Instandhaltungsarbeiten ein klares, gesetzlich verankertes Zutrittsrecht zu fremden Grundstücken. Dieses Betretungsrecht muss im Notfall auch für Flächen ohne vordefinierten räumlichen Bezug zu betroffenen Leitungen und Anlagen gelten, da im Vorfeld nicht abzuschätzen ist, wo eine Störung auftritt und wie sie behoben werden kann. Nur so können Leitungen und Anlagen schnell wiederhergestellt werden. Der rechtliche Rahmen kann im EnWG geschaffen werden, wo bereits Betretungs- und Leitungsrechte normiert sind (vgl. § 44 oder § 48a EnWG). So würde für alle Beteiligten ein rechtssicherer Rahmen geschaffen, unter dem die Inanspruchnahme fremder Grundstücke unter klar definierten Voraussetzungen möglich ist.

Genehmigungspflichten für Notfallmaßnahmen abschaffen bzw. konzentrieren

Reparaturarbeiten und provisorische Wiederherstellungsmaßnahmen sollten grundsätzlich von energiewirtschaftsrechtlichen Genehmigungspflichten freigestellt sein. Fachrechtliche Einzelgenehmigungen (zum Beispiel nach Wasser- oder Naturschutzrecht) sollten, wo möglich, entfallen oder in stark beschleunigten Verfahren erteilt werden. Anknüpfungspunkte bieten unter anderem das Infrastrukturzukunftsgesetz, das Reparaturmaßnahmen bereits von Genehmigungen ausnimmt. Wo eine Freistellung nicht möglich ist, sollte eine weitgehende Konzentration der Rechtsgrundlage von Genehmigung und Organisation im Katastrophenfall angestrebt werden.

Schwerlasttransporte schnell und unbürokratisch ans Ziel bringen

Dringlichen Schwerlasttransporten von kritischen Betriebsmitteln (zum Beispiel Transformatoren oder Mastprovisorien) sollte im Notfall Vorrang vor anderen Schwerlasttransporten und der üblichen Nutzung der Verkehrsinfrastruktur eingeräumt werden, gegebenenfalls auf Anordnung der Bundesregierung beziehungsweise der zuständigen Aufsichtsbehörden. Dieser Vorrang muss bei Bedarf auch durch Polizeibegleitung zum Zielort durchgesetzt werden können.

FORDERUNGEN

Außerdem sollten im Notfall Ausnahmegenehmigungen zur Befahrung von Brücken und anderen begrenzten Fahrwegen gelten. Hintergrund ist, dass statische Auslastungsgrenzen auf dauerhafte Verkehrsbelastungen ausgelegt sind und nicht auf einmalige Schwerlasttransporte im Krisenfall. Übliche Vorgaben für Großtransporte wie zum Beispiel das Sonntagsfahrverbot, Betretungsverbote, oder Umweltschutzauflagen sollten befristet ausgesetzt werden können, soweit der Schutz von Personen und die Transportsicherheit gewährleistet sind.

Mit Übungen und Abstimmungen für ein pragmatisches Verwaltungshandeln sorgen

Einsatz, Errichtung, Betrieb und Transport von Notfallbetriebsmitteln sollten zwischen Bund, Ländern und Netzbetreibern abgestimmt werden, um Handlungsspielräume und Befugnisse frühzeitig abzustecken. Offene Rechtsfragen müssen frühzeitig im Dialog mit den zuständigen Behörden geklärt werden, um im Ernstfall schnell handlungsfähig zu sein. Auf Ebene der Bundesländer sollten konkrete Einsatzszenarien und Katastrophenschutzpläne entwickelt werden, die – insbesondere in der Verkehrsplanung und -steuerung – die Belange der Netzbetreiber bzw. des Stromnetzes berücksichtigen. Die Szenarien müssen im Sinne der Krisenprävention regelmäßig gemeinsam geübt werden.

Strategische Notreserve für kritische Betriebsmittel prüfen

In Ergänzung der unternehmensinternen Lagerhaltung sollte der gesetzlich geregelte Aufbau einer strategischen Notreserve an kritischen Betriebsmitteln (zum Beispiel Transformatoren) geprüft werden, um nach Angriffen oder Sabotageakten schnell alternative Versorgungslösungen bereitstellen zu können. Die Kosten für die strategische Notreserve müssen regulatorisch anerkannt werden (siehe hierzu auch Kapitel 11).

SCHUTZ, ÜBERWACHUNG UND DATENVERARBEITUNG ANLAGENBEZOGEN STÄRKEN

5 ÜBERWACHUNG DER EIGENEN ASSETS PRAGMATISCH ERMÖGLICHEN

AUSGANGSLAGE

Netzbetreiber sind auf moderne Überwachungsinstrumente angewiesen, um Sabotage, Ausspäh- und Einbruchsversuche frühzeitig zu erkennen und darauf reagieren zu können. Während fremde beziehungsweise feindliche Drohnen sich nicht an rechtliche Vorgaben halten, sind eigene Drohnen der Netzbetreiber – etwa für Inspektionen und Überwachung – durch strikte Genehmigungspflichten und Datenschutzvorgaben stark eingeschränkt. Das führt zu einer faktischen Asymmetrie zulasten der Verteidiger Kritischer Infrastrukturen – denn mit dem Betriebspersonal allein ist ein großflächiges Netzgebiet nicht zu überwachen.

FORDERUNGEN

BVLOS-Drohnenflüge für KRITIS-Betreiber erleichtern

Für Betreiber Kritischer Infrastrukturen sollten Beyond-Visual-Line-of-Sight-Drohnenflüge (BVLOS) zur Remote-Überwachung des gesamten Netzes aus zentralen Leitstellen möglich sein. Ziel ist eine Erreichbarkeit aller Netzabschnitte innerhalb von weniger als einer Stunde durch geeignete Überwachungsmittel. Insbesondere kleinteilige und umfassende Antragspflichten für die einzelnen Drohnenflüge beim Luftfahrt-Bundesamt oder bei den zuständigen Landesbehörden verhindern jedoch de facto die flächendeckende Nutzung von Drohnen zur Netzüberwachung. Genehmigungen sollten nicht mehr an begrenzte Zeiträume und Fluggebiete gebunden sein. Erforderlich ist die Schaffung eines Erlaubnistatbestandes für KRITIS-Betreibern zur angemessenen Überwachung ihrer Anlagen – entlang von Freileitungen beispielsweise innerhalb eines eingegrenzten Luftraums rund um die Leitungen. Nur so bekommen Netzbetreiber die Augen, die sie brauchen.

Videoüberwachung und Drohnendetektion erleichtern

Die umfassende Videoüberwachung insbesondere von Umspannanlagen und Stromtrassen (Freileitung und Erdkabel) und der Einsatz von Drohnendetektion (inklusive aktiver Radarkomponenten) sollten für KRITIS-Betreiber rechtlich privilegiert und unbürokratisch genehmigungsfähig sein. Dazu braucht es umfassende Erleichterungen im Datenschutzrecht, da an vielen Stellen das Filmen des öffentlichen Raums und die Speicherung von personenbezogenen Daten erforderlich sind.

Gefahrenabwehr ist eine hoheitliche Aufgabe

Derzeit wird viel über die Einbindung der KRITIS-Betreiber in die aktive Gefahrenabwehr diskutiert – was in letzter Konsequenz eine Aufweichung des staatlichen Gewaltmonopols wie zum Beispiel Drohnenabschüsse bedeuten würde. Diese Debatte ist aus der Sicht von Amprion jedoch nicht von praktischer Relevanz. Der gesetzliche Auftrag der Übertragungsnetzbetreiber sieht eine operative Rolle in der Gefahrenabwehr nicht vor. Vielmehr braucht es umfassende Möglichkeiten zur Überwachung der eigenen Assets, um im Ernstfall die Sicherheitsbehörden schnell zu verständigen und die Reaktionsfähigkeit zu erhöhen.

6 KLAREN RECHTSRAHMEN FÜR DATENVERARBEITUNG UND DATENSCHUTZ SCHAFFEN

AUSGANGSLAGE

Videoüberwachung und Drohnendetektion erfordern die Verarbeitung personenbezogener Daten. Derzeit stützen sich KRITIS-Betreiber häufig auf das „berechtigte Interesse“ als Rechtsgrundlage, was in jedem Einzelfall abwägungsbedürftig und rechtlich angreifbar ist. Speicherfristen sind nicht einheitlich geregelt und werden von Gerichten unterschiedlich bewertet. Dies erschwert aufgrund massiver rechtlicher Unsicherheiten die zwingend erforderliche flächendeckende Videoüberwachung der Anlagen. KRITIS-Betreiber dürfen nicht gezwungen sein, zwischen der Einhaltung von Datenschutzrecht und dem Schutz Kritischer Infrastrukturen abzuwägen. Der Gesetzgeber sollte klare Prioritäten und Vorgaben formulieren, um Rechtssicherheit herzustellen.

FORDERUNGEN

Spezifische Erlaubnistatbestände für KRITIS-Datenverarbeitung schaffen
Die Umsetzungsverordnungen des KRITIS-Dachgesetzes und flankierende Regelungen (KRITIS-DG- und BSIG-Umfeld) sollten eindeutige Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Kontext von Videoüberwachung, Drohnendetektion und -flügen sowie anderen sicherheitsrelevanten Technologien wie beispielsweise KI-Unterstützung bei der Bilddatenauswertung schaffen.

Verlängerte Speicherfristen rechtssicher ermöglichen
Für sicherheitsrelevante Daten (zum Beispiel Videoaufzeichnungen an Stationen, Drohnenbilder) sollten gesetzlich verlängerte Speicherfristen sowie klare Vorgaben zur Auswertung und Weitergabe festgelegt werden. Dadurch können Vorfälle erkannt, analysiert und abgewehrt werden, ohne in rechtliche Unsicherheiten zu geraten.

7 OBJEKTSCHUTZ UND ANLAGENHÄRTUNG VON GENEHMIGUNGSPFLICHT BEFREIEN

AUSGANGSLAGE

Vor dem Hintergrund der verschärften Bedrohungslage müssen bestehende und neue Anlagen des Stromnetzes (Umspannanlagen, Leitungen, Kabelaufführungsmasten) baulich besser geschützt werden. Hierzu gehören (höhere) Zäune, verstärkte Tore, Einhausungen beispielsweise von Transformatoren oder Kabelabgängen, Videoüberwachung oder die Härtung von Betriebsgebäuden. Derzeit führen baurechtliche Bestimmungen (zum Beispiel Baugenehmigungspflicht und Abstandsflächen) und immissionsschutzrechtliche Verfahren vielfach zu Verzögerungen, auch wenn es sich um reine Schutzmaßnahmen ohne zusätzliche Belastungen handelt.

FORDERUNGEN

Umspannanlagen von der Baugenehmigungspflicht freistellen
Die Landesbauordnungen sollten so angepasst werden, dass Anlagen, die der allgemeinen Versorgung mit Elektrizität dienen (insbesondere Umspannanlagen), weitgehend von der Baugenehmigungspflicht freigestellt werden.

FORDERUNGEN

Die Regelung für verfahrensfreie Anlagen sollte ohne Größenbeschränkung gelten. Dies würde zum einen das Genehmigungsverfahren nach dem Bundes-Immissionsschutzgesetz (BImSchG), welches in der Regel bei Umspannanlagen Anwendung findet und etwaige Baugenehmigungen einschließt, vereinfachen und beschleunigen. Zum anderen könnten einzelne Baumaßnahmen, die keiner Genehmigungspflicht nach dem BImSchG unterliegen, verfahrensfrei durchgeführt werden. Diese Regelung würde sowohl für bereits bestehende als auch neu zu errichtende Umspannanlagen Objektschutzmaßnahmen erheblich erleichtern.

Nebenanlagen ohne Abstandsflächen zulassen
Schutzanlagen wie Zäune, Toranlagen und Einhausungen sollten als Nebenanlagen von Abstandsflächenregelungen ausgenommen werden.

Transformatorentausch beschleunigen
Der Austausch von Transformatoren – meist gegen modernere und leistungsstärkere Geräte – sollte nach dem Vorbild von § 3 Nr. 1 NABEG durch Genehmigungsfreistellungen oder Verfahrenserleichterungen vereinfacht werden, sofern die neuen Transformatoren mit der gleichen Auslastung weiterbetrieben werden. Dies betrifft sowohl immissionsschutzrechtliche Änderungsgenehmigungen als auch gegebenenfalls erforderliche Baugenehmigungen.

INFRASTRUKTUR UND NETZPLANUNG RESILIENT UND FINANZIERUNGSSICHER GESTALTEN

8 VERKEHRSINFRASTRUKTUR ALS VORAUSSETZUNG FÜR RESILIENZ STÄRKEN

AUSGANGSLAGE
Die Resilienz der Strominfrastruktur hängt unmittelbar von der Leistungsfähigkeit der Verkehrsinfrastruktur ab. Kritische Ersatzteile und Großgeräte mit teilweise mehreren Hundert Tonnen Gewicht erreichen ihren Einsatzort nur dann, wenn Straßen, Brücken, Bahntrassen, Binnenwasserstraßen und Häfen in einem Zustand sind, der Schwerlasttransporte zulässt. Heute sorgen Engpässe in vielen Bereichen für eine stark limitierte Routenwahl und verlängerte Transportzeiten.

FORDERUNGEN

Belange des Stromnetzes bei der Verkehrsplanung berücksichtigen
Maßnahmen zur Instandsetzung und Instandhaltung von Straßen, Brücken, Tunneln, Bahntrassen, Schleusen und Hafenanlagen sollten so ausgerichtet werden, dass für den Transport kritischer Betriebsmittel möglichst mehrere nutzbare Routen verfügbar sind. Die Bedeutung der Verkehrsinfrastruktur für die sichere Stromversorgung sollte in der verkehrspolitischen Prioritätensetzung berücksichtigt werden.

FORDERUNGEN

Es ist zwingend erforderlich, dass die zuständigen Verkehrsbehörden auf Bundes- und Länderebene regelmäßig mit Netzbetreibern zusammenkommen, um die Bedarfe der Netzbetreiber in der Verkehrsplanung zu berücksichtigen.

Wegeinfrastruktur für Schwerlasttransporte von Großgerät auslegen
Insbesondere für Transformatorentransporte und andere Großgeräte ist eine vorausschauende Anpassung der Verkehrsinfrastruktur erforderlich, um ad hoc notwendige Transporte nicht an Engstellen oder mangelnden Tragfähigkeiten scheitern zu lassen.

9 RESILIENZORIENTIERTE NETZPLANUNG ERMÖGLICHEN

AUSGANGSLAGE
Die geltenden gesetzlichen Vorgaben zur Netzplanung sind stark auf Effizienz und Minimierung des Netzausbaus ausgerichtet. Eine vorausschauende Netzplanung, die über das netztechnisch Notwendige hinausgeht und so die Resilienz systematisch stärkt, ist nur sehr eingeschränkt möglich. Gleichzeitig zeigt sich angesichts wachsender Einspeisung erneuerbarer Energien, zunehmender Elektrifizierung und neuer Bedrohungslagen, dass Redundanzen und gezielte Verstärkungen kritischer Assets volkswirtschaftlich sinnvoll sein können. Resilienz wird bislang in der Kosten-Nutzen-Bewertung von Netzausbaumaßnahmen nicht explizit berücksichtigt.

FORDERUNGEN

Resilienzfaktor und Geo-Redundanz in die Netzplanung integrieren
Der Netzentwicklungsplan (NEP) sollte um einen expliziten Resilienzfaktor ergänzt werden. Dieser ermöglicht begrenzte, gezielte Redundanzen und die Verstärkung kritischer Assets, ohne die Effizienzanforderungen grundsätzlich aufzugeben. Konkrete kritische Elemente sind dabei nicht öffentlich auszuweisen. Zudem sollte das Bündelungsgebot im Planungsrecht geöffnet werden. Für besonders kritische Netzelemente wird so eine Geo-Redundanz ermöglicht.

Handlungsspielräume für Leistungsreserven ermöglichen
Bei der Planung des Übertragungsnetzes darf nicht gegenüber anderen Belangen überschießend geplant werden (Vorratsplanung). Es fehlt an Festlegungen, welche Ereignisse und Störungsszenarien planerisch und betrieblich abzusichern sind. Es sollten Spielräume für die Planbegründung von Vorhaben geschaffen werden, sodass eine vorausschauende Planung erfolgen kann, um im Falle von benötigten Leistungserhöhungen keine zusätzliche Genehmigung einholen zu müssen. Die Umsetzung von Leistungsreserven in definierten Grenzen würde das Stromnetz zukunftsfester machen.

10 KRITISCHE INFRASTRUKTUR BEI KONKURRIERENDEN VORHABEN PRIORISIEREN

AUSGANGSLAGE

Der Ausbau und die Ertüchtigung der Netzinfrastruktur sind die Grundvoraussetzung für eine sichere Stromversorgung und das Gelingen der Energiewende. Zwar werden zahlreiche Vorhaben als „im überragenden öffentlichen Interesse“ eingestuft, doch umfasst dieser Status sehr unterschiedliche Projekttypen (zum Beispiel Netzausbau, EE-Anlagen und Batteriespeicher). Bei Abwägungen in Planungs- und Genehmigungsverfahren und bei Flächenkonflikten fehlt damit häufig eine klare Priorisierung.

FORDERUNGEN

Vorrang von Netzausbauvorhaben gesetzlich klarstellen
Maßnahmen der Netzinfrastruktur sollten bei konkurrierenden Vorhaben im überragenden öffentlichen Interesse ausdrücklich vorrangig berücksichtigt werden. Ihnen sollte ein eigenständiger, besonders gewichtiger Abwägungsbelang zugewiesen werden.

Prioritäre Bearbeitung durch Behörden verankern
Genehmigungsbehörden sollten verpflichtet werden, Vorhaben der Übertragungsnetzbetreiber, die der Stabilität und Versorgungssicherheit dienen, vorrangig zu bearbeiten und zügig zu bescheiden.

Stationsprojekte angemessen privilegieren
Umspannanlagen sind die Drehscheiben im Stromnetz und zentrale Knotenpunkte der Stromversorgung. Stationsprojekte, die bislang nicht oder nur begrenzt gesetzlich privilegiert sind, sollten umfassend als Maßnahmen im überragenden öffentlichen Interesse eingestuft werden und entsprechenden Vorrang erhalten.

11 FINANZIERBARKEIT, KOSTENANERKENNUNG UND LIEFERKETTEN FÜR KRITISCHE KOMPONENTEN SICHERN

AUSGANGSLAGE

Resilienz ist nicht zum Nulltarif zu haben. Investitionen in zusätzliche Redundanzen, Lagerhaltung, Sicherheitsmaßnahmen und Personal erhöhen dauerhaft die Kosten der Übertragungsnetzbetreiber. Diese erwartbar erheblichen Belastungen können ohne eine klare Finanzierungsperspektive andere dringend erforderliche Projekte verdrängen und so den Netzausbau verzögern. Gleichzeitig sind Lieferketten für kritische Komponenten (insbesondere Transformatoren) bereits heute angespannt. Dies ist nicht nur eine Hypothek für den Netzausbau, sondern auch für Überlegungen zur verstärkten Lagerhaltung solcher Betriebsmittel.

FORDERUNGEN

Finanzierung und öffentliche Mittel für ein resilientes Stromnetz berücksichtigen
Erwartbar hohe Aufwendungen für Resilienzmaßnahmen müssen für die Übertragungsnetzbetreiber risikoneutral refinanzierbar sein. Die Refinanzierung muss regulatorisch vollständig und ohne Zeitverzug möglich sein. Resilienzmaßnahmen dürfen zudem nicht zu vermeintlichen Ineffizienzen und damit zu wirtschaftlichen Nachteilen für die Netzbetreiber führen. Dies umfasst Investitionen in die Netzinfrastruktur, dezentrale Lagerhaltung und erhöhten Betriebsaufwand (OPEX). Zur Finanzierung könnten gegebenenfalls Mittel aus dem Sondervermögen Infrastruktur oder dem Verteidigungshaushalt – auch als Beitrag zur Erreichung des NATO-Verteidigungsziels – beitragen.

Lieferketten durch politischen Branchendialog stärken
Transformatoren und andere kritische Komponenten sollten durch einen politisch unterstützten Branchendialog langfristig abgesichert werden. Dazu gehört auch die Prüfung von Zwischenlagerkonzepten und der Ausbau von Produktionskapazitäten in Europa.

Schwerlasttransportkapazitäten berücksichtigen
Neben der Komponentenproduktion müssen auch Kapazitäten im Schwerlasttransport in den Blick genommen und langfristig gesichert werden.

KOOPERATION, ZUGRIFFSRECHTE UND INFORMATIONSAUSTAUSCH AUSBAUEN

12 KRISENPRÄVENTION: AUSTAUSCH UND ÜBUNGEN MIT SICHERHEITSBEHÖRDEN INTENSIVIEREN

AUSGANGSLAGE
Netzbetreiber kennen die eigenen Infrastrukturen und Verwundbarkeiten am besten, sind aber häufig von sicherheitsrelevanten Informationen abgeschnitten. Umgekehrt sind Betreiber und ihre Anlagen vor Ort nicht immer hinreichend in die Einsatzplanung der Sicherheitsbehörden eingebunden. In Krisenlagen kann dies zu Informationsdefiziten und Zugangsproblemen an Unfall- und Katastrophenorten führen, wie beispielsweise beim Ahrtal-Hochwasser oder bei einem Chemiepark-Unfall in Leverkusen sichtbar wurde. Dies führte in letzter Konsequenz zu kritischen Verzögerungen von Entstörungsarbeiten.

FORDERUNGEN

Gesetzliche Grundlagen für Informationsweitergabe nutzen und ausbauen
Verfassungsschutzgesetze sollten eine frühzeitige Informationsweitergabe an KRITIS-Betreiber ermöglichen – auch bei abstrakten Gefährdungslagen. Das Beispiel des neuen Verfassungsschutzgesetzes NRW (§ 3 Abs. 1 Nr. 3 VSG NRW) kann als Vorbild dienen.

FORDERUNGEN

Operativen Austausch mit Polizei und Sicherheitsbehörden verstärken
Regelmäßige Austauschformate, gemeinsame Lagebewertungen und Übungen sollten dazu beitragen, dass Netzbetreiber, Polizei und weitere Sicherheitsbehörden (BOS) einander kennen, Zugang zu Anlagen in Krisenlagen gewährleistet ist und Abläufe eingeübt sind. Zukünftig sollte sichergestellt werden, dass technischem Personal von Amprion während polizeilicher Maßnahmen der Zugang zu Unfallorten gewährt wird, um Sicherungs- und Reparaturarbeiten durchführen zu können. Dafür ist auch die polizeiliche Begleitung des Betriebspersonals zu Unfallorten erforderlich. Dementsprechend ist die Sensibilisierung der Innenministerien und Polizeidirektionen der Länder eine wichtige Voraussetzung. In einem weiteren Schritt sollten alle relevanten Standorte der Netzbetreiber bei den jeweils zuständigen Polizeidienststellen hinterlegt werden. Nicht zuletzt braucht es die Einbindung der Übertragungsnetzbetreiber in eine schwarzfallfeste Kommunikation mit den BOS.

13 ZUGRIFFSRECHTE DER ÜBERTRAGUNGSNETZBETREIBER AUF DATEN UND NETZELEMENTE SICHERSTELLEN

AUSGANGSLAGE
Die Steuerbarkeit dezentraler Energieanlagen (insbesondere EE-Anlagen und Batteriespeicher) ist für die Systemsicherheit zentral. Obwohl gesetzliche Anforderungen an die Steuerbarkeit bestehen, ist die Steuerbarkeit im Verteilnetz mangels technischer Umsetzung sowie Smart-Meter-Rollout inklusive Steuereinrichtung nicht flächendeckend gegeben. Für Übertragungsnetzbetreiber ist es jedoch von zentraler Bedeutung, ein möglichst echtzeitnahes Bild von Erzeugung und Verbrauch über das eigene Netzgebiet und bis in unterlagerte Netzebenen zu haben, um den Systembetrieb jederzeit sicher gewährleisten zu können. Gleichzeitig entstehen zentrale Herstellerplattformen (zum Beispiel Wechselrichter-Apps), über die potenziell tief in das Energiesystem eingegriffen werden kann.

FORDERUNGEN

Durchsetzung der Steuerbarkeit sicherstellen
Bereits bestehende Anforderungen zur Steuerbarkeit von EE-Anlagen und Speichern müssen konsequent umgesetzt werden. Dazu braucht es klare Verantwortlichkeiten und technische Mindeststandards im Verteilnetz.

Europäische Betreiberpflichten für Herstellerplattformen
Zentrale Plattformen zur Steuerung dezentraler Anlagen sollten innerhalb der EU betrieben werden und starken Sicherheitsanforderungen unterliegen. Hersteller und Dritte dürfen keinen unkontrollierten Einfluss auf das Energiesystem erhalten.

Zugriffsmöglichkeiten der ÜNB auf relevante Daten verbessern
Übertragungsnetzbetreiber sollten – in Abstimmung mit Verteilnetzbetreibern – ausreichende Zugriffsrechte auf netz- und systemrelevante Daten erhalten, um ihre Systemverantwortung auch in einem dezentralen Energiesystem wahrnehmen zu können.

14 EUROPÄISCHE DIMENSION DER RESILIENZ STÄRKEN

AUSGANGSLAGE

Das Stromnetz ist ein europäisch integriertes Verbundsystem – Störungen und Angriffe machen daher nicht an Staatsgrenzen halt. Gleichzeitig stellt das kontinentale Verbundnetz die Stromversorgung auf breitere Füße und macht das Stromnetz resilienter. Interkonnektoren, grenzüberschreitende Zusammenarbeit und gegenseitige Hilfe sind zentrale Pfeiler der europäischen Dimension der Resilienz. Derzeit entsteht in Europa eine Vielzahl neuer Regulierungsansätze[1].

FORDERUNGEN

Transparenzpflichten überprüfen und neue Transparenzvorgaben durch EU-Sicherheits- und Resilienzvorgaben vermeiden

Auch auf europäischer Ebene besteht der Auftrag, bestehende und künftige Transparenz und Veröffentlichungspflichten (zum Beispiel in den Richtlinien (EU) 2022/2555 (NIS2) und 2022/2557 (CER)) systematisch daraufhin zu überprüfen, ob sie sicherheitsrelevante Informationen in unangemessener Detailtiefe öffentlich zugänglich machen.

Network Codes Grid Connection schnell überarbeiten

Seit 2022 läuft die Überarbeitung der Codes (Recast) wegen technologischer Entwicklungen beziehungsweise der Zunahme von PV, Wind, Batterien, Elektrolyseuren und Sektorkopplung. Nach der Konsultation durch ENTSO-E und ACER wurde der Vorschlag Ende 2023 an die Kommission übermittelt. Die Europäische Kommission hat im Juni 2025 angekündigt, die Annahme der neuen Verordnungen auf unbestimmte Zeit zu verschieben. Diese Verzögerung birgt erhebliche Risiken für Versorgungssicherheit und Interoperabilität. Zudem führen nationale Zwischenlösungen zu Fragmentierung und höheren Kosten.

Regulatorische Harmonisierung anstreben

NIS2, NCCS und nationale Umsetzungen sollten möglichst harmonisiert und Doppelregulierung vermieden werden – beispielsweise mit Blick auf die Regelungen zu kritischen Komponenten. Nationale Alleingänge schwächen die Resilienz des gemeinsamen europäischen Stromnetzes.

Europäische Sicherheitstechnologien und IT-Souveränität fördern

Die Informations- und Kommunikationstechnik (IKT) bildet das Nervensystem des Stromnetzes. Jüngste globale Konflikte haben eindrücklich vor Augen geführt, dass außereuropäische Abhängigkeiten gerade bei Komponenten der Kritischen Infrastruktur die betriebliche Sicherheit im Stromnetz schwächen können. Europäische Hersteller von Sicherheitstechnologien sollten gezielt gestärkt werden, um Abhängigkeiten von außereuropäischen Marktführern zu reduzieren. Gleiches gilt für den Aufbau souveräner europäischer Cloud-Infrastrukturen, auf die Netzbetreiber bei sensiblen Daten zurückgreifen können.

[1]Die Europäische Kommission hat für Mai 2026 eine Revision des Energy Security Framework angekündigt. Im Zuge dieser Veröffentlichung bereitet Amprion ein vertieftes Positionspapier zu der europäischen Dimension einer resilienten kritischen Strominfrastruktur vor.

FORDERUNGEN

Standardisierung und Fachkräfteentwicklung
Die Ausbildung von Fachkräften – insbesondere im Leitungsbau und in der Informationssicherheit – sollte auf europäischer Ebene unterstützt werden. Für Krisenfälle sind erleichterte Einreiseregeln und schnelle Anerkennung von Qualifikationen für ausländische Fachkräfte zu prüfen.

Europäische Regelwerke für den Netzbetrieb anpassen
Europäische Vorgaben wie die System Operation Guideline sollten so weiterentwickelt werden, dass eine einheitliche Praxis der europäischen Übertragungsnetzbetreiber im Umgang mit Störungen (unter anderem Fehlerbegrenzung und Spannungsbandhaltung) möglich wird. Erfahrungen aus vergangenen Störungen, wie etwa der Blackout auf der Iberischen Halbinsel im Jahr 2025, sollten kontinuierlich einfließen.

IMPRESSUM

Redaktion:
Jonas Lewe, Niklas Tenberge

Kontakt:
landespolitik@amprion.net,
politik@amprion.net

Amprion GmbH
Juni 2026