

Akademie für Politik und Zeitgeschehen

ECKPUNKTE ZUR ENERGIEWENDE I 2026

Die Sicherheit unserer Energieinfrastrukturen



Im Jahr 2017 setzten sich Experten auf Einladung der Hanns-Seidel-Stiftung und in Zusammenarbeit mit dem Wirtschaftsbeirat Bayern in einem zweitägigen Workshop mit dem Stand der Energiewende in Deutschland auseinander: Ihr Ziel: notwendige Weichenstellungen identifizieren. Der Teilnehmerkreis: Vertreter aus Wirtschaft, Politik, Beratung und Wissenschaft. Das Diskussionsergebnis wurde in einem gemeinsamen Eckpunktepapier festgehalten. Der „Bernrieder Kreis zur Energiewende“ wurde fortgeführt. Folgende Eckpunkte stehen zur Verfügung:

Bernrieder Kreis, 2025: „**Flexibilitätsoptionen**“.

Das Energiesystem der Zukunft erfordert eine Bandbreite an Flexibilitätsoptionen - der Schlüssel für Versorgungssicherheit, Netzstabilität und Kosteneffizienz. [Eckpunkte Flexibilitätsoptionen \(pdf\)](#)

Bernrieder Kreis, 2023 „**Inkonsistenzen**“.

Überlegungen zu Grundprinzipien einer konsistenten Energiewende und Beispiele für Inkonsistenzen als Impuls für einen als notwendig erachteten Analyseprozess. [Eckpunkte Inkonsistenzen \(pdf\)](#)

Bernrieder Kreis, 2022 „**Eckpunkte zur Energieversorgungssicherheit in Bayern**“.

Reduzierung der Risiken beim Energieimport, Ausbau der erneuerbaren Energien und Begleitmaßnahmen [Eckpunkte Energieversorgungssicherheit \(pdf\)](#)

Bernrieder Kreis, 2020 Sondersitzung „**Grundsätze 2020**“.

Trotz allen Willens, die Gefahr des Scheiterns besteht. Identifizierung der Faktoren. [Grundsätze zur Energiewende \(pdf\)](#)

Bernrieder Kreis, 2019 „**Der Steuerungsansatz der Energiepolitik**“.

Kriterien für eine effektive Lenkungswirkung mit dem primären Ziel, Treibhausgas-Emissionen zu reduzieren. [Eckpunkte Steuerungsansatz \(pdf\)](#)

Bernrieder Kreis, 2018: „**Regional erzeugte Energie regional nutzen**“.

Wie regionale Energiegemeinschaften zu definieren sind und als Baustein der Versorgungssicherheit funktionieren können. [Eckpunkte Regionale Energien \(pdf\)](#)

Bernrieder Kreis, 2017: „**Schlüsselfragen der Energiewende**“.

Grundsätzliche Anmerkungen und notwendige Weichenstellungen in den Bereichen Steuern, Umlagen und Abgaben, Stromnetze und Netzstruktur, Versorgungssicherheit, Sektorenkopplung und Energieeffizienz, Gesetzgebung. [Schlüsselfragen \(pdf\)](#)

Sicherheit unserer Energieinfrastrukturen Resilienz für unsere Energieversorgung Zukunftsfähigkeit unseres Wirtschaftsstandorts

Das Eckpunktepapier stellt zunächst dar, dass Energieinfrastrukturen als „Lebensadern“ der Gesellschaft zu „Kritischen Infrastrukturen“ gehören, deren Schutz und Sicherheit für die Stabilität von Wirtschaft, Gesellschaft und Staat besonders relevant sind.

Zunächst werden kurz Gefahren für Energieinfrastrukturen skizziert – diese reichen von Naturkatastrophen über technische Störungen bis hin zu physischen und digitalen Angriffen sowie geopolitischen Risiken.

Zentrale Gegenmaßnahmen sieht der Bernrieder Kreis in robusten Anlagen und Reserven, klaren Zuständigkeiten, regelmäßigen Krisenübungen und in einer besseren nationalen und europäischen Zusammenarbeit. Besonders betont werden dezentrale Energiesysteme, lokale Notversorgung und höhere Energieeffizienz, weil sie Ausfälle begrenzen und die Wiederherstellung erleichtern. Langfristig sollen Deutschland und Europa unabhängiger bei Rohstoffen, Technologien und Fachwissen werden und Investitionen in eine widerstandsfähige Energieversorgung stärker fördern.

Angesichts des technologischen Wandels auf globaler Ebene, wie der Digitalisierung und Elektrifizierung sowie des KI-Einsatzes, und vor dem Hintergrund eines neuen geopolitischen Umfeldes mit neuen Versorgungs- und Sicherheitsrisiken, ist eine neue Sicherheitskultur notwendig. Investitionen in die Resilienz kritischer Infrastrukturen sind nicht nur eine Voraussetzung für die künftige Versorgungssicherheit, sondern auch ein strategischer Bedingungsfaktor für die künftige technologische und industrielle Wettbewerbsfähigkeit und somit in die Zukunftsfähigkeit des Wirtschaftsstandort Deutschlands.

INHALT

PRÄAMBEL	4
Energie als Kritische Infrastruktur.....	4
Resilienz als Schlüsselbegriff	5
Sicherheit als Investition in die Zukunftsfestigkeit	5
Wo liegen die Gefahren?	6
Was können wir tun?	9
Vorsorge durch Robustheit der Anlagen und Reserven	9
Überwachung und Sicherheit.....	9
Notbetrieb und Wiederherstellung	9
Bevorratung für lokale Krisenfälle	10
Bevorratung auf nationaler Ebene	10
Europäischer Verbund	10
Vorbereitung auf effektive Krisenbewältigung.....	11
Koordination auf nationaler Ebene gewährleisten.....	11
Kapazitäten auf lokaler Ebene koordinieren.....	11
Sicherheitskultur in der Bevölkerung entwickeln	12
Mit dezentralen Systemen und Effizienz die Resilienz des Gesamtsystems erhöhen	12
Die Chancen eines dezentralen, zellulären Energiesystems nutzen	12
Energieeffizienz voranbringen	13
AUSBLICK: Fortlaufende Verbesserung sicherstellen	14
Mehr Unabhängigkeit und Souveränität schaffen	14
Know-how halten und aufbauen	14
Aus Erfahrungen lernen.....	14
Rahmenbedingungen durch Regulierung und Finanzierung setzen	15
Finanzierungspotenziale nutzen	15

PRÄAMBEL

Ende Januar 2026 verabschiedete der Bundestag das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (kurz „KRITIS Dachgesetz“). Es trat nach Zustimmung des Bundesrats Mitte März in Kraft. Ziel ist, die Resilienz kritischer Infrastrukturen durch verbindliche Pflichten, Mindeststandards, Meldeprozesse und eine gestärkte Aufsicht systematisch zu erhöhen. Das Gesetz muss nun durch Rechtsverordnungen konkretisiert werden.

Mit den Eckpunkten zeigen wir exemplarisch auf, welche Aspekte im Energiebereich dabei hineinspielen können.

Energie als Kritische Infrastruktur

Deutschland hängt stark von sicheren Infrastrukturen zur Daseinsvorsorge ab. Ausfälle können weitere Versorgungssysteme stören oder gar zum Erliegen bringen.

Die Energieversorgung ist dabei besonders kritisch, da sie Bedingung für den Betrieb aller kritischen Infrastrukturen und vieler anderer Sektoren ist. Zentrale Bereiche des Alltags, der Wirtschaft und des Staates bauen darauf auf, etwa Information und Kommunikation, Transport und Verkehr, Wasserversorgung und –entsorgung, medizinische Versorgung, Verwaltung oder Finanzwesen. All diese Bereiche zählen zu den kritischen Infrastrukturen, die für das Funktionieren der Gesellschaft besonders wichtig sind (▶ siehe KRITIS, in: BBK).

Für die Stabilität und Versorgungssicherheit stellen insbesondere wechselseitige Abhängigkeiten zwischen einzelnen Teilsystemen ein Risiko dar, da Störungen dadurch kaskadenartig weitergegeben werden können.

Das Internet ist abhängig von Strom, etwa für Rechenzentren, Mobilfunkmasten, Glasfasernetze und Router. Gleichzeitig ist die Energieversorgung zunehmend digital gesteuert. Kraftwerksanlagen, Stromnetze, Umspannwerke und Gasspeicher etc. nutzen IT-Systeme zur Überwachung und Steuerung.

Ob Klimawandel oder Geopolitik: Die Entwicklungen der letzten Jahre machen uns bewusst, dass diese Infrastrukturen - im Ausland, aber auch im Inland - verwundbar sind und dass wir sie noch besser schützen müssen (s.u. „Mögliche Gefahren“)¹. Bedrohungen der Energieinfrastrukturen sind kein abstraktes Szenario, sondern Realität². Die Energieversorgung so aufzustellen, dass Schäden nur zu minimierten Ausfällen führen, sollte strukturell und konsequent implementiert werden.

Mehr denn je gilt: Energiepolitik ist Wirtschafts- und gleichzeitig Sicherheitspolitik zur Wahrung gesamtgesellschaftlicher und gesamtstaatlicher Sicherheit und Stabilität³.

1 Siehe auch ▶ Studie Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), 2011 „Was bei einem Blackout geschieht“

2 Siehe Frank Umbach “Strategic Vulnerabilities: Hybrid Warfare Threats from Russia and China on Europe’s Critical Infrastructures”, ▶ europe.hss.de Global Perspectives, 26 August 2025

3 Siehe Aussage „Die Versorgungssicherheit ist auch eine Frage der nationalen Sicherheit“ im Rahmen der ▶ VKU-Forderung (link) nach dem Anschlag auf die Strominfrastruktur in Berlin am 3. Januar 2026.

Resilienz als Schlüsselbegriff

Resilienz ist hier ein Schlüsselbegriff: er beschreibt die Fähigkeit, Krisen durchzustehen und zu bewältigen. Dabei kann man unterschiedliche Phasen und Bewältigungstiefen unterscheiden: von kurzfristigen und lokalen Maßnahmen des Krisenmanagements und der Wiederherstellung („zurück zum Normalzustand“), über die Abwehr, Milderung und Vermeidung von Krisen bis hin zu Anpassung und langfristigen Systemveränderungen⁴ mit neuen Denkweisen und Sicherheitskulturen – also Lösungen, die ineinandergreifen und als Gesamtheit gedacht werden.

Sicherheit als Investition in die Zukunftsfestigkeit

Investitionen in die Resilienz kritischer Infrastrukturen und Versorgungssicherheit sind auch Investitionen in zusätzliche Wettbewerbsfähigkeit und in die Zukunftsfähigkeit des Wirtschaftsstandort Deutschlands. Der Umbau unserer Energieversorgung ist in diesem Sinne zugleich ein Weg zur Stärkung der geopolitischen Unabhängigkeit und der Versorgungssicherheit.

⁴ Vgl. hierzu ► [BDEW-Diskussionspapier](#) (pdf), August 2025: „Resilienz im Energiesektor: Handlungsfelder und –bedarfe“ oder ► [VKU-Papier](#) zum Wintervorfall in Berlin vom 8.1.2026

Wo liegen die Gefahren?

Unsere Energieinfrastrukturen – also alle Anlagen, die der Erzeugung, Speicherung und Verteilung von Energie dienen - sind von zentraler Bedeutung. Unterschiedlichste Gefahren können ihre Sicherheit bedrohen, etwa:

Naturkatastrophen und Klimawandel

Hochwasserereignisse, Stürme oder Waldbrände zerstören oder beschädigen Anlagen physisch wiederholt europaweit. Damit ist in Zukunft laut Klimamodellen verstärkt zu rechnen. Hitze- und Dürreperioden mit Niedrigwasser wirken sich auf die Leistungsfähigkeit von Wasserkraftanlagen, Kernkraftwerken, Wasserstraßen und Kühlsystemen aus. Große Hitze, aber auch Vereisungen und schwere Schneemassen, bringen Stromleitungen an ihre Grenzen.

(Material-)Technische und organisatorische Risiken

Materialermüdung, Überlastung, Fehlfunktionen, Bedienfehler können zu technischen Störungen, zum Ausfall von einzelnen Anlagen und über Kettenreaktionen sogar zu Blackouts führen.

Personalmangel bei Netzbetreibern, Behörden und Unternehmen, unklare Zuständigkeiten, mangelhafte Notfallpläne und zu wenig Simulationen und Übungen sowie Engpässe bei Material, Ersatzteilen oder Brennstoffen sind weitere Risiken.

Angriffe auf Energieinfrastrukturen

Insbesondere Anlagen der Kritischen Infrastruktur (KRITIS) sind potenzielle Angriffsziele von Terroranschlägen oder im Kriegsfall.

Hierzu zählen gezielte Anschläge auf z.B. Windparks, Stromleitungen, Pipelines, Umspannwerke oder LNG-Terminals. Zu erinnern sei hier etwa an die Sprengstoffanschläge auf die Nord-Stream-Pipelines am 26. September 2022. Der Brandanschlag auf zwei Strommasten am 9. September 2025 führte in Berlin zu einem großflächigen Stromausfall, was gewaltbereiten Linksextremisten zugeschrieben wird⁵. Auch mutmaßlich von Russland gesteuerte Angriffe nehmen zu⁶. Vandalismus und Diebstahl im großen Stil (z.B. Module von PV-Freiflächenanlagen oder Kupferleitungen) können ebenfalls Elemente im System beeinträchtigen.

Cyberattacken

Der globale Anstieg von ausgeklügelten Cyberangriffen ist alarmierend.

In der Energieversorgung von heute sind die physischen Infrastrukturen eng mit digitalen Mess-, Überwachungs-, Kommunikations- und Steuerungssystemen verbunden. Angriffe in Form von Spionage, Manipulation oder Destabilisierung können daher unmittelbare Auswirkungen auf den realen Anlagen- und Netzbetrieb haben. Manipulierte Messwerte oder unterbrochene Datenübermittlung etwa könnten falsche Leistungsanforderungen, Regelungseingriffe oder Schaltaktionen auslösen.

5 Siehe ► www.verfassungsschutz.de link zu Website „Angriffe von Linksextremisten auf Kritische Infrastrukturen und Wirtschaftsunternehmen“, Stand Januar 2026

6 Das Bundesamt für Sicherheit in der Informationstechnik - BSI, aber auch die NATO, die EU und westliche Geheimdienste, gehen davon aus, dass auch unsere **Energieanlagen** Angriffsziele hybrider Kriegführung Russlands sind. Siehe z.B. auch ► www.verfassungsschutz.de link zu pdf „Gefährdungen durch russische Spionage, Sabotage und Desinformation“ vom Mai 2025

Im Zuge der Energiewende gibt es mehr dezentrale Erzeugungsanlagen. Einerseits bedeutet das weniger „Single-Points-of-Failure“, andererseits aber mehr steuerbare Verbraucher wie Wärmepumpen, Wallboxen und Batteriespeicher, mehr Smart Meter und Kommunikationsschnittstellen, Echtzeitdaten und Fernwartungspunkte sowie Abhängigkeiten von Cloudanbietern oder Programmierschnittstellen. All dies sind potenzielle Angriffspunkte, die prinzipiell auch kaskadenartigen Auswirkungen auf das Gesamtenergiesystem oder andere Sektoren haben können.

Kombination aus physischen und digitalen Angriffen

Besonders kritisch ist die Kombination von physischen und digitalen Angriffen (womöglich mit Insiderwissen). So können Cyberangriffe zunächst der Ausspähung von Anlagen, Netzstrukturen und Betriebsabläufen dienen und zu einem späteren Zeitpunkt gezielt für Sabotage genutzt werden. Umgekehrt können physische Schäden an Strom- oder Kommunikationsverbindungen dazu führen, dass digitale Überwachungs-, Schutz- und Steuerungssysteme nicht mehr verfügbar sind.

Geopolitische Risiken

Konflikte in Regionen mit wichtiger Energieproduktion wirken sich direkt bei uns aus. Die Abhängigkeit betrifft nicht nur Import- und Lieferländer, sondern auch Transitstaaten. Hier drohen Risiken durch Angriffe auf Pipelines, Seekabel, Offshore-Anlage oder Schiffe.

Darüber hinaus wirken sich Sanktionen, Handelskonflikte oder politische Erpressung auf Liefermengen und Preise aus.

Abhängigkeitsrisiken – bei fossilen Rohstoffen

Lange wurde die Abhängigkeit fossiler Rohstoffe insbesondere im Zusammenhang mit der Rohstoffknappheit als Problem wahrgenommen (Endlichkeit der förderbaren Quellen). Aktuell wird deutlich, dass auch die globalen Transportwege einzubeziehen sind, da sie den fortlaufenden Versorgungsfluss von Kraft- und Brennstoffen unmittelbar betreffen. Die unter Beschuss stehenden Meerengen „Straße von Hormus“ und „Bab al-Mandab“ bei Yemen, der der 2021 durch einen querstehenden Tanker blockierte Suezkanal, die Sprengungen 2022 an der Nord-Stream-Pipeline, aber auch die durch Zölle und Sanktionen limitierten Transporte zeigen, wie sich globale Bedrohungen wirtschaftlich, fiskalisch und gesellschaftlich auf uns auswirken können.

Abhängigkeitsrisiken⁷ – bei Erneuerbaren Energien

Das System der Erneuerbaren Energien ist zwar nicht von täglichen Lieferströmen abhängig, doch die Anlagen selbst - etwa Windkraftträder und Solaranlagen - benötigen durchaus kritische Rohstoffe, z.B. Seltenen Erden und weitere Metalle wie Lithium und Kupfer.

Dabei geht es nicht nur um die natürlichen Vorkommen und ihre technologische Nutzbarkeit. Weitere Risiken können Widerstände gegen den Abbau sein oder die Übernutzung von Ressourcen, insbesondere bei Biomasse. Besonders problematisch ist, wenn die Vorkommen der erforderlichen Rohstoffe auf einige wenige Länder beschränkt sind. Insbesondere China nimmt bei der Förderung und Weiterverarbeitung kritischer und strategischer Rohstoffe eine dominante Stellung ein und hat sich zudem den Zugriff auf entsprechende Minen im Ausland langfristig gesichert – und somit eine Voraussetzung seiner Politik der strategischen Kontrolle ganzer Liefer- und Wertschöpfungsketten künftiger Schlüsseltechnologien und Zukunftsindustrien.

Darüber hinaus dominiert China Technologien und Produkte inklusive Software-Komponenten, die für die Energiewende von zentraler Bedeutung sind, etwa Akkus, Solarpanels oder Wechselrichter. Abgesehen davon, dass über Ausfuhrbeschränkungen oder Zölle ein Druckmittel aufgebaut werden kann, besteht dabei auch die Gefahr, dass hier aufgestellte Anlagen von den Herstellern in der Ferne gesteuert werden – ein mögliches Einfallstor für gezielte Manipulationen (s.o.).

⁷ Siehe auch Frank Umbach „Energie- und Sicherheitspolitik. Warum wir eine vernetzte Sicherheitspolitik benötigen“, in: APuZ 46-47/2022, S. 8-15 ► www.bpb.de

Gesellschaftliche und politische Gefahren

Der Widerstand der Bevölkerung kann den Bau wichtiger Energieanlagen enorm verzögern und verteuern und politische Ziele und Umsetzungsschritte beeinflussen. Solche politisch-gesellschaftlichen Akzeptanzprobleme verringern nicht zuletzt die Planungssicherheit und Investitionsbereitschaft der Unternehmen.

Erschwerend kommen gezielte Desinformation und Propaganda durch bestimmte politische Gruppen hinzu, die den Klimawandel oder die Notwendigkeit der Energiewende leugnen. Dies kann zu Vertrauensverlust der Bevölkerung in Infrastrukturbetreiber oder Staat führen, was auch notwendige Vorsorge- und Sicherheitsmaßnahmen unterminiert.

Wechselwirkungen und Kettenreaktion

Besonders problematisch wird die Situation dann, wenn ein Systemausfall auch andere Systeme betrifft, weil es dann „Rettungsaktionen“ umso mehr erschwert: Ein Ausfall digitaler Kommunikationsnetze ist unter Umständen auch mit einem Ausfall der Steuerung der Energienetze verbunden. Werden in einem Katastrophenfall wichtige Verkehrsachsen behindert, trifft dies auch notwendige Brennstoff- oder Ersatzteillieferungen. Ein Cyberangriff bei Extremwetter, wenn technische Hilfs- und Rettungsdienste im Einsatz sind, löst personelle Engpässe aus und blockiert notwendige Koordinierungsleistungen. Wo Wasserversorgung oder Kanalisation ausfällt, fehlt binnen Tagesfrist unsere zentrale Lebensgrundlage und gewohnte hygienische Bedingungen sind schwer aufrechtzuerhalten.

Was können wir tun?

Um mit derartigen Schocks und Krisen besser umgehen zu können, gilt es die Robustheit von Anlagen und Systemen zu fördern (z.B. sichere Standards, starker Schutzmantel). Aus der Resilienzforschung weiß man, dass auch Redundanzen (Vorhalten gleichwertiger Ersatzkomponenten oder –pfade, die beim Ausfall der regulären Elemente einspringen können) und Rückfallstrategien (die Fähigkeit, wieder auf vorige Modelle zurückgreifen zu können, falls neue Technologien nicht genutzt werden können) hilfreiche Elemente sind, um im Schadensfall einen Notbetrieb oder raschen Wiederaufbau zu gewährleisten. Netzwerke oder koordinierte dezentrale Einheiten verhindern, dass ein System durch einen einzigen Angriff komplett lahmgelegt wird, und eröffnen durch eine höhere Diversität und Agilität mehr Reaktionsspielraum.

Vorsorge durch Robustheit der Anlagen und Reserven

Überwachung und Sicherheit

Energieinfrastrukturen befinden sich oft in der Peripherie bzw. lassen sich nur schwer physisch beispielsweise durch Zäune oder Bunker schützen.

Die Raumordnung bis hin zu Landes- und Regionalplanung muss Sicherheitsfragen in dem neuen geopolitischen Umfeld einer viel instabileren multipolaren Weltordnung kritisch mitdenken und in ihre Abwägungen einpflegen. So ist beispielsweise die Bündelung verschiedener Infrastrukturen (etwa Verkehrs- und Energieleitungen) einerseits flächensparend, könnte andererseits aber auch zeitgleiche Angriffe auf verschiedene Ziele erleichtern. Dies gilt es zu bedenken. Gleichzeitig sind Transparenzpflichten beispielsweise in Planfeststellungsverfahren kritisch zu hinterfragen, werden doch wichtige Parameter (wie z.B. von Netzknoten) auch online leicht einsehbar.

Um Schäden oder Manipulationen frühzeitig zu erkennen und Maßnahmen der Abwehr ergreifen zu können, ist ein Monitoring notwendig, etwa über eingebaute Echtzeitsensorik und Powerline-Überprüfungen oder Überwachungsdrohnen.

Für digitale Komponenten sollten hohe Sicherheitsstandards gelten (Cyber-Sicherheit).

Es wird zunehmend Fachkräfte für Sicherheits- und Resilienzberatung benötigen, daher sollten Akkreditierungsverfahren, anerkannte Beratungsstandards für Risikoanalysen und Resilienzpläne sowie klare Schnittstellen zwischen behördlicher Aufsicht und externer Fachexpertise geschaffen werden.

Notbetrieb und Wiederherstellung

Wichtige Anlagen und Systeme im Energiesystem, aber auch in den Kommunen und Unternehmen müssen im Schadensfall weiter funktionieren. Die Technik dafür ist in der Regel vorhanden – es ist eine Frage der Abstimmung und Organisation. Daher muss das Wissen über Handlungsoptionen und Reaktionsmöglichkeiten und darüber hinaus die Befähigung zur Umsetzung vorhanden sein (s.u.).

Die Reparierbarkeit von Anlagen sollte bereits bei ihrer Auswahl und Ausgestaltung eine Rolle spielen. Die unterschiedlichen Anlagentypen haben jede für sich verschiedene Vor- und Nachteile, die sorgfältig abgewogen werden müssen. Bei den Stromleitungen zum Beispiel wären Freileitungen leichter wiederherstellbar; Erdleitungen dagegen womöglich weniger leicht angreifbar.

Bevorratung für lokale Krisenfälle

Kommunen stehen vor der Herausforderung, dass im Notfall, etwa Stromausfall, wichtige Einrichtungen wie Stadtwerke oder Krankenhäuser weiter funktionieren. Sie müssen daher Reservekapazitäten wie „Unterbrechungsfreie Stromversorgung“ und Notstromaggregate vorhalten.

Zur Gewährleistung der Instandhaltung sollte darüber hinaus auch ein Vorrat an Ersatzteilen (einschl. Strom- und Internetkabeln) gelagert werden, statt sich auf just-in-time-Lieferungen zu verlassen.

Die lokale Ebene wird jedoch nicht alles vorhalten können, hier würden „Resilienz-Cluster“ Sinn machen, also eine koordinierte, regionale Bevorratung. Eine zuvor definierte Stelle muss allerdings die Verantwortung innehaben und die Beschaffungssituation überblicken und auch die Koordination eines Teams übernehmen, das in einer Krisenlage die Kapazität hat, die Wiederherstellung in Angriff zu nehmen.

Notlösungen wie der „Dieselgenerator“ sind nach wenigen Stunden oder Tagen erschöpft. Sind auch noch Transportwege blockiert, wird ein Nachschub schwer zu organisieren sein. Dezentrale erneuerbare Anlagen haben den Vorteil, lokal zur Verfügung zu stehen. Mit neuen, heutigen Technologien, die vielfach bereits unverbunden vorhanden sind, können daraus Infrastrukturen gebaut werden (→s.u. Abschnitt „Zellulare Systeme“), die im Normalbetrieb ihren Dienst leisten und im Ernstfall die Krisendienste entlasten. Jede „Insel“, die im Falle eines Blackouts funktioniert, hilft dem Gesamtsystem.

Bevorratung auf nationaler Ebene

Die Gefahr besteht, dass eingeplante Importmengen nicht geliefert werden können - etwa aufgrund geopolitischer Entwicklungen oder jahreszeitlicher Bedingungen. Verlässlich gefüllte Gas- und Kraftstoffspeicher werden daher weiterhin benötigt, v.a. im Winter. Hier können wir von anderen Ländern lernen, etwa Frankreich, das seine Gasspeicher schützt und die Befüllung durch Anreizregulatorik sicherstellt.

Die Gaspipelines bieten nicht nur gute Transportmöglichkeiten („grüner“ Moleküle wie Biomethan oder Wasserstoff) sondern auch Speichermöglichkeiten. Sie sollten daher in künftige Energiesysteme eingebunden werden

Europäischer Verbund

Die Vernetzung mit Nachbarstaaten über Interkonnektoren spielt eine entscheidende Rolle für die Versorgungssicherheit Deutschlands und ist Voraussetzung eines stabilen EU-Energiebinnenmarktes. Das Stromnetz und die Gasinfrastrukturen sollten daraufhin überprüft werden, ob sie die im Krisenfall geplanten Solidaritätsmaßnahmen länderübergreifend ermöglichen, zum Beispiel durch reverse flow-Kapazitäten und durch den Ausbau bilateraler Strominterkonnektoren zwischen den EU-Mitgliedsstaaten (wie z.B. zwischen Spanien und Frankreich sowie in Osteuropa).

Der Ausbau der Energiepartnerschaften zwischen der EU und anderen Ländern, die den energie- und klimapolitischen Weg der EU ergänzen, kann zusätzlich dazu beitragen, die Versorgung mit kritischen und systemrelevanten Rohstoffen zu sichern, wobei gleichzeitig entsprechende Importkapazitäten geschaffen werden müssen. Leuchtturmprojekte mit politischer Flankierung und finanzieller Unterstützung können helfen, konkrete Projekte rasch in die Umsetzung zu bringen. Da etwa die USA seit 2025 bereits eine Vielzahl neuer Importlieferverträge mit Ländern aus allen Teilen der Welt unterschrieben haben, sollte hier ebenfalls zügig gehandelt werden, denn der Konkurrenzdruck steigt.

Vorbereitung auf effektive Krisenbewältigung

Koordination auf nationaler Ebene gewährleisten

Im Ernstfall müssen alle wissen, was zu tun ist, von der vertikalen Verantwortungskette bis zur horizontalen Ebene der ressortübergreifenden Zusammenarbeit.

Im „klassischen Katastrophenfall“ ist dies weitestgehend strukturiert. Im militärischen Krisenfall sowie durch hybride Bedrohungen ist die Lage noch nicht so klar. Betreiber und Kommunen sollten regelmäßig strukturierte Krisenszenarien durchspielen, die realistische Kombinationen aus physischer Sabotage, Cyberangriff und Kommunikationsausfall abbilden - statt nur Einzelrisiken, wie im Katastrophenschutz üblich.

Solche Szenario-Übungen sollten drei Ebenen einbeziehen:

- Technische Wiederherstellung
Wer repariert was, mit welchen Ersatzteilen, transportiert auf welchen Wegen?
- Kommunikation
Wie informiert man Bevölkerung und Presse bei Ausfall der üblichen Kanäle?
- Zuständigkeitsklärung
Wer entscheidet, wenn Landkreis, Land und Bund gleichzeitig betroffen sind?

Der Berliner Blackout vom Januar 2026 hat gezeigt, dass genau diese Schnittstellen in der Praxis oft ungeklärt sind, was im Krisenfall wertvolle Zeit kostet (siehe Positionspapiere von VKU und BDEW in Fußnoten 2 und 3).

Ein Praxisbeispiel für gelungene vertikale und horizontale Koordination liefert das Baltikum: Litauen hat den Schutz seiner wichtigsten Energieanlagen von privaten Betreibern auf staatliche Sicherheitsbehörden übertragen, um die Synchronisierung mit dem europäischen Stromnetz und die Abkopplung von Russland und Belarus im Februar 2025 abzusichern. Diese Entkopplung wurde von einer verstärkten Überwachung kritischer Seekabel und Interkonnektoren begleitet, koordiniert zwischen NATO, EU und den drei baltischen Staaten.

Für Deutschland heißt das: Die Sicherheitsverantwortung für besonders kritische Netzelemente, wie Umspannwerke, Interkonnektoren und LNG-Terminals, sollte in einem klar definierten, abgestuften Modell zwischen Betreiber, Landespolizei/-behörden und Bund geklärt und verankert werden.

Zuständigkeiten und eine klare Rollenverteilung sind entscheidend, damit jeder im Ernstfall weiß, was zu tun ist. Energiesicherheit ist zunehmend eine bilaterale und europäische Koordinationsfrage, nicht nur eine nationale.

Kapazitäten auf lokaler Ebene koordinieren

Reservisten und ehrenamtlich tätige Personen, die etwa beim Technischen Hilfswerk, in der Freiwilligen Feuerwehr oder im Rettungswesen aktiv sind, spielen im Krisenfall eine besondere Rolle. Für Unternehmen ist allerdings wichtig zu wissen, wo ihr Personal dann eingesetzt wird – als Maschinist im Unternehmen selbst oder als Kommandant der gemeindlichen Feuerwehr im Umfeld – welche Hierarchie bzw. „Unabkömmlichkeit“ gilt im Einsatzfall? Dies ist festzulegen. Unternehmen müssen (datenschutzrechtlich) berechtigt sein, sich hierüber einen Überblick zu verschaffen.

Sicherheitskultur in der Bevölkerung entwickeln

Es braucht einen gesamtgesellschaftlichen Bewusstseinswandel⁸. Themen, wie Sicherheit und geopolitische Zusammenhänge, wurden lange verdrängt. Die Auffassung „hier wird schon nichts passieren“, „mich betrifft es schon nicht“ oder „ich bin ja versichert“ könnte sich jedoch als Trugschluss erweisen. Denn die Folgen des Klimawandels sind real, die geopolitischen Spannungen und Krisenherde nehmen zu, und manche Risiken werden nicht (mehr) versicherbar sein.

Auch in den eigenen vier Wänden gilt es, ein Mindestmaß an Vorsorge und Bevorratung zu treffen, wie auch vom BSI empfohlen. Wie repariere ich ein defektes Gerät? Das allgemeine Verständnis, wie damalige und heutige Elemente, die zur Daseinsvorsorge notwendig sind, funktionieren, kann in Krisensituationen helfen.

Mit dezentralen Systemen und Effizienz die Resilienz des Gesamtsystems erhöhen

Dezentrale Systeme und eine höhere Energieeffizienz entlasten das Gesamtsystem im Krisenfall.

Die Chancen eines dezentralen, zellulären Energiesystems nutzen

Ein System, das aus wenigen großen zentralen Einheiten besteht, birgt das Risiko, dass mit nur wenigen Angriffen große Bereiche lahmgelegt werden. Ein System, das aus vielen kleinen unabhängigen Einheiten besteht, ist demgegenüber robuster⁹.

Im Ideal werden die Einheiten (Zellen) so angelegt, dass sie im Bedarfsfall über Synergien vor Ort das System von unten nach oben stützen und wiederaufbauen können. Fällt eine einzelne Anlage oder Leitung aus, bleibt der Schaden auf eine begrenzte Zelle beschränkt. Andere Zellen können ihren Betrieb eigenständig fortsetzen und sich gegenseitig stützen. Damit sinkt die Gefahr großflächiger Versorgungsunterbrechungen erheblich.

Diese Dezentralität schafft Redundanz, reduziert kritische (Import-)Abhängigkeiten und erhöht die Reaktionsfähigkeit im Störfall. Ein solches System ist für Angriffe unattraktiver, da relevante Schäden einen höheren Einsatz des Angreifers /Saboteurs erfordern, als mit zentralen Einheiten flächendeckend zu schädigende Systeme¹⁰.

Regionale Erzeugungsanlagen, Speicher und flexible Verbraucher verkürzen Transportwege, verringern die Abhängigkeit von überregionalen Netzen und ermöglichen es, lokale Lasten auch bei Störungen oder Engpässen weiterhin zu versorgen. Können einzelne Energiezellen im Inselbetrieb arbeiten und ihre Betriebsführung auf physikalischen Messgrößen aufbauen, bleiben wesentliche Funktionen selbst dann erhalten, wenn Kommunikationsnetze oder zentrale Leitsysteme eingeschränkt sind.

8 Vgl. Benjamin Hahn/ Bohdana Chepka: Kein Bevölkerungsschutz ohne Bevölkerung , ► [HSS Policy Paper 1/2026](#) pdf.

9 Das Institut für Technikfolgenabschätzung hielt bereits 2011 in der ► [Studie „Was beim Blackout geschieht“](#) fest: „Unter Nutzung dezentraler vernetzter Stromerzeuger könnten regional begrenzte Inselnetze nach einem Stromausfall weiterhin Strom erzeugen. Bereits ein punktueller, auf öffentliche Einrichtungen mit hoher Bedeutung für die Katastrophenbewältigung beschränkter Auf- und Ausbau von Inselnetzen – insbesondere auf der Basis regenerativer Energien – könnte eine Stärkung der Resilienz der Stromversorgung und damit der Kritischen Infrastrukturen bewirken“ (S. 29 f).

10 Angesichts der aktuellen Angriffe auf die zentralen Großkraftwerke setzt die Ukraine aktuell tatsächlich verstärkt auf dezentraler erneuerbare Systeme („Small, distributed renewable assets can provide a more resilient alternative to large, centralised fossil fuel assets“ in: Energy is the new frontline of security: Lessons from Ukraine’s battle-tested system 16. Januar 2026, ► [World Economic Forum](#)).

Ein zellulares Energiesystem ersetzt das bestehende Verbundnetz nicht, sondern entwickelt es weiter¹¹. Die Vernetzung vieler autonomer Einheiten schafft ein Gesamtsystem, das sich an veränderte Rahmenbedingungen anpassen kann, Ausfälle besser verkraftet und nach Störungen schneller wieder in einen stabilen Betrieb zurückkehrt. Die verschiedenen Netzebenen müssen aber eng zusammenarbeiten.

Die Betriebsweise und das Management (Steuerung) der Netze sollten dahingehend weiterentwickelt werden. Es geht hier nicht um die Abschaffung bestehender Netze und Betriebsstrukturen, sondern darum, mehr Möglichkeiten zur Stärkung eines resilienten Energiegesamtsystems zu erschließen.

Die Eigenversorgung (z.B. von Unternehmen oder Quartieren) sollte in diesem Sinne attraktiver werden, denn verbrauchsnahe Erzeugung vermeidet Transportwege (Netze) und erhöht damit die Resilienz der Versorgung vor Ort. Dabei geht es nicht um eine Entkoppelung und Entsolidarisierung vom gemeinschaftlichen Energienetz, sondern um eine Steigerung der Flexibilität und Unabhängigkeit. Das stärkt den Einzelnen und das Gesamtsystem.

Jedes Gebäude, das – wenn auch nur in Teilen - energieautark bleiben kann, ist ein Gewinn im Sinne der Resilienz.

Energieeffizienz voranbringen

Regionale, dezentrale Erzeugungsanlagen und Speichersysteme bringen zusammen mit Elektrifizierung und Effizienzsteigerung der Verbraucher ein erhebliches Potential für die Steigerung der Resilienz des Gesamtsystems.

Anlagen, die wenig andere Energieinfrastruktur oder Brennstoffe brauchen (z.B. Wasserkraft, Geo-, Solarthermie, Wärmepumpen), reduzieren die nötige Zahl von Anlagen kritischer Infrastruktur und bieten somit strukturell weniger Angriffspunkte, die Sicherheitslösungen erfordern.

Eine hohe Energieeffizienz von Systemen ermöglicht insbesondere in Kombination mit elektrischen und nichtelektrischen Energiespeichern eine (lange) Überbrückung von Ausfällen oder Engpässen der Energieversorgung.

Beispiele: Ein besonders gut gedämmtes Kühlhaus mit großer Menge an kalten Gebäudemassen oder Kühlgut kann nach einem Stromausfall auch ohne Notstromaggregat noch lange kühl bleiben. Analog können gut gedämmte Gebäude bei Stromausfall im Winter längere Zeiten ohne Heizung überbrücken.

11 Vgl. ► [VDE Studien](#) „Der zellulare Ansatz“ von 2015, „Das zellulare Energiesystem“ von 2019 und „Das zellulare Verteilnetz“ von 2026.

AUSBLICK: Fortlaufende Verbesserung sicherstellen

Mehr Unabhängigkeit und Souveränität schaffen

Um unabhängiger von globalen Lieferketten zu werden und die Wertschöpfung im Lande zu behalten, sollte überprüft werden, inwiefern lokale Energiequellen erschlossen werden können, etwa Biokraftstoffe wie Biomethan und Bioöle oder Geothermie. Es sollte dabei auch nicht ausgeschlossen werden, heimische Gasquellen stärker zu erschließen (, wie dies etwa Rumänien oder Griechenland, tun) oder gegebenenfalls natürlichen „weißen Wasserstoff“ zu nutzen.

Um die Abhängigkeiten von Rohstoffen und Technologien anderer Länder zu reduzieren, sollten eigene Lösungen geschaffen werden, etwa

- Beteiligung an Minen oder Erschließung eigener Minen oder Verbesserung der Kreislauffähigkeit.
- Eigene Erzeugung von Komponenten.
- Diversifizierung im IT- System („Windows und Linux“) und bei Clouds bzw. digitale Souveränität.
- Bessere Regelungen und Verschlüsselungen oder Vermeidung von Steuerungselementen (Hard-/ Software), die von Externen manipuliert werden könnten.
- Eigene Programmierung und Aufbau von Kapazitäten, um die Systeme zu verwalten.

Know-how halten und aufbauen

Das Augenmerk gilt auch dem Bereich der „Human Capacity“, den es zu erhalten bzw. erst noch zu schaffen gilt, beispielsweise

- Ingenieurskapazitäten im eigenen Land bzw. in Europa halten und vor Abwanderung sichern, damit im Krisenfall ausreichend Wissen vorhanden ist, das z.B. für die Reparatur von Anlagen benötigt wird.
- Wissen und Forschung auch in den Bereichen erhalten, die aufgrund der Energiewende abgebaut werden (z.B. Kernkraft und Kohleabbau), deren Umsetzbarkeit derzeit als schwierig gilt (z.B. Carbon Capture und Storage/CCS) oder die in den letzten Jahren ins Ausland verlagert wurden (z.B. Solarzellenproduktion). Denn es kann Situationen geben, in denen das Wissen wieder gebraucht wird, weil neue Forschungsergebnisse und Technologien die bisherigen Risiken relativieren oder weil äußere Umstände dazu zwingen, eigene Ressourcen und Produktionsmöglichkeiten wieder zu nutzen.
- Wissen in Zivilgesellschaft aufbauen, wie man sich in Krisen behelfen kann (Vorsorge etwa durch eigene Bevorratung mit Batterien; Umsetzung von Notlösungen, wie Heizen mit Holz oder Aufbereitung von Brauchwasser; Fähigkeit, auch neuere Technologien wie Wärmepumpen reparieren zu können).

Aus Erfahrungen lernen

Die Lehren aus dem russischen Angriffskrieg gegen die Ukraine sollten genutzt werden, um Angriffsmuster und effiziente Schutz- und Verteidigungsoptionen besser zu verstehen¹².

Die baltischen Staaten sehen ihre Energieinfrastruktur seit der Abkopplung vom russisch-belarussischen Stromnetz 2025 einem deutlich höheren Bedrohungsniveau ausgesetzt und haben ihre Schutzkonzepte für Seekabel, Strominterkonnektoren und Umspannwerke entsprechend angepasst. Diese Erfahrungen sind näher an einer möglichen deutschen Realität als oft angenommen, da ähnliche hybride Angriffsmuster (Ankerwurf-Sabotage an Kabeln, koordinierte Cyber-Physical-Angriffe) bereits gegen deutsche und westeuropäische Ziele konstatiert wurden und weiter zunehmen.

¹² Vgl. Webbericht von Yuriy Honcharenko / Yurii Mindyuk: „Blackout in Kyjiw - Stromnetz im Visier“

► www.hss.de, 03.03.2026

Ein regelmäßiger, strukturierter Austausch von “Best Practices” und “Lessons Learned” mit baltischen und osteuropäischen Sicherheitsbehörden und Netzbetreibern sollte daher institutionalisiert werden - als kontinuierliches Frühwarn- und Lernnetzwerk, das Bedrohungsmuster identifiziert, bevor sie in Deutschland eintreten.

Erfahrungen aus Katastrophengebieten wie dem Ahrtal (Hochwasser-Katastrophe 2021) sollten genutzt werden, um nicht nur das Katastrophenmanagement (Warnsysteme, Rettungsmaßnahmen etc.) zu verbessern oder den Ort wiederaufzubauen, sondern auch, um sich im Sinne der Resilienz zu fragen, inwiefern ein umfassender Wandel stattfinden muss. Vielleicht sollte man beispielsweise nicht mehr an allen riskanten Orten eine Bebauung zulassen, eine Versicherung ist ohnehin oft nicht mehr möglich. Versicherungen sollten den Wiederaufbau dann an anderer Stelle als versichert einbeziehen, auch in Bestandsverträgen.

Rahmenbedingungen durch Regulierung und Finanzierung setzen

Jenseits der technischen Lösungen müssen die regulatorischen Anforderungen einem modernen System entsprechend gestaltet und die derzeit noch vorhandenen Verzerrungen abgebaut werden. Besonders die energiewirtschaftlichen gesetzlichen Grundlagen müssen dem Wandel hin zu einem resilienten Energiesystem folgen und geeignete Anreize für die Marktakteure liefern. Das Marktdesign muss so gestaltet werden, dass systemdienliches Verhalten stärker belohnt wird. Systemdienlichkeit und marktwirtschaftliche Instrumente müssen dafür integriert und harmonisiert werden. Um systemdienliche Investitionen anzureizen, können neue Finanzierungs- und marktorientierte Instrumente eingeführt werden.

Finanzierungspotenziale nutzen

Um nicht nur die Herausforderungen der Klimaanpassung und der Energiewende zu meistern, sondern auch den gestiegenen Sicherheitsbedürfnissen gerecht und die Chancen der Resilienz nutzen zu können, müssen zusätzliche Gelder mobilisiert und die Finanzierungsinstrumente weiterentwickelt werden¹³.

Resiliente Energieinfrastrukturen sind nicht nur eine Sicherheitsaufgabe, sondern eine strategische Investition in Versorgungssicherheit, wirtschaftliche Wettbewerbsfähigkeit und die Zukunftsfähigkeit Deutschlands!

13 Ein Vorschlag ist der Aufbau eines „eigenkapitalstärkenden Energiewende-Fonds (EWF)“ zur Finanzierung der Energiewende (siehe ► [“Kapital für die Energiewende“ BDEW VKU Deloitte, 2024](#)). der gezielt da zum Einsatz kommen soll, wo bisherige Förderungs- und Finanzierungslösungen ausgereizt sind und das Risiko-Rendite-Profil durch staatliche Maßnahmen gestützt werden sollte.“

Die Ausführungen in dem vorliegenden Papier erheben keinen Anspruch auf Vollständigkeit. Sie sind als Hinweise zu einzelnen Punkten der Energiediskussion zu verstehen, sind aber nicht Positionen der Organisationen der Teilnehmer.

Der Dank für die wertvollen Impulse geht an alle Teilnehmer dieser Expertenrunde, die sich vom 11.-12. Juni 2026 mit dem Thema auseinandersetzte; für die Mitwirkung am Papier insbesondere an

Niclas von Ambüren (Partner BlueRock Security & Resilience Strategies GmbH)

Dr. Norbert Ammann (Referatsleiter Umwelt, Energie, Klima, IHK München und Oberbayern)

Josef Bayer (Geschäftsführer EnSolVision GmbH)

Gunnar Braun (Geschäftsführer VKU Landesgruppe Bayern)

Dr. Stefan Burger (Dezernent Kraftstoffe, Energieversorgung, Wehrwissenschaftliches Institut für Werk- und Betriebsstoffe)

Dr. Josef Hochhuber (Ministerialbeamter für Grundsatzfragen erneuerbarer Energien)

Dr. Christoph Rapp (Leiter Wasserkraft, SWM Stadtwerke München)

Dr. Andreas Schieder (Senior Advisor Public Affairs and Communications, Political Affairs GE Tennet)

Anna Schwamberger (Referentin Vorstandsbüro & Politik bayernwerk)

Dr. Frank Umbach (Forschungsleiter EUCERS/ CASSIS, Universität Bonn)

Dr. Ralf Wagner (Lead Market Analyst, Uniper Global Commodities)

Prof. Dr. Andreas Zeiselmaier (Professur für Digitale Energiewende, Hochschule Weihenstephan-Triesdorf)

Silke Franke

Referentin für Umwelt, Energie,
Städte und Ländlicher Raum der
Akademie für Politik und Zeitgeschehen
Hanns-Seidel-Stiftung

Telefon: 089 1258-226

E-Mail: franke@hss.de

Bernrieder Kreis

Denkfabrik der Hanns-Seidel-Stiftung zur Energiepolitik