
Resilienz als Machtfrage: Angriff auf die Infrastruktur

Von JULIA ENGELS

Wenn im Winter Umspannwerke brennen, Kraftwerksblöcke ausfallen und Hochspannungsleitungen zerfetzt am Boden liegen, richtet sich die Gewalt nicht bloß gegen technische Anlagen. Vielmehr trifft sie Wohnungen, Pflegeheime, Operationssäle, Schulen - kurz: die elementaren Voraussetzungen zivilen Lebens.¹ Die russischen Angriffe auf die ukrainische Energieinfrastruktur haben damit in aller Deutlichkeit vor Augen geführt, was in hoch entwickelten Gesellschaften häufig unsichtbar bleibt: Energie ist nicht bloß ein ökonomischer Produktionsfaktor. Sie ist die infrastrukturelle Grundlage moderner Existenz. Ohne Strom funktionieren weder Krankenhäuser noch Kommunikationsnetze, weder Verkehrssteuerung noch Wasserversorgung.

Die Zerstörung von Energieinfrastruktur trifft daher nicht allein technische Systeme. Sie trifft das gesellschaftliche Leben selbst. Zeitweise waren 1,2 Millionen Haushalte in der Ukraine nach massiven russischen Angriffen ohne Stromversorgung.² In stark elektrifizierten Gesellschaften bedeutet ein längerer Stromausfall nicht lediglich Unannehmlichkeiten, sondern eine fundamentale Störung der sozialen Ordnung. Genau darin liegt die strategische Wirkung solcher Angriffe.

Der Krieg wirkt hier wie ein Brennglas. Er macht sichtbar, wie stark moderne

Gesellschaften von komplexen technischen Systemen abhängen und wie verwundbar diese Systeme zugleich sind. Stromnetze, Wärmekreisläufe, Wasseraufbereitung, digitale Kommunikation und Logistik bilden ein dichtes Geflecht gegenseitiger Abhängigkeiten. Diese Systeme sind hochgradig effizient, präzise austariert und im Normalbetrieb erstaunlich stabil. Aber ausgerechnet diese Effizienz erzeugt eine paradoxe Form der Verletzbarkeit. Denn je enger Systeme miteinander verzahnt sind, desto stärker können lokale Störungen systemweite Folgen entfalten.

Damit verschiebt sich die strategische Logik gegenwärtiger Konflikte. Wo früher industrielle Zentren oder militärische Anlagen im Mittelpunkt standen, rücken aktuell die unsichtbaren Infrastrukturen des Alltags ins Visier. Elektrizität, Datenströme und Wärmeversorgung bilden gewissermaßen das Nervensystem moderner Gesellschaften. Wird dieses Nervensystem angegriffen, entstehen Effekte, die weit über die unmittelbare Zerstörung hinausreichen. Der Schaden liegt nicht allein im zerstörten Transformator, sondern im Ausfall eines ganzen Systems, das Millionen Menschen zugleich betrifft.

Die Energiearchitektur des 20. Jahrhunderts folgte einem klaren Paradigma: große Kraftwerke, weiträumige Übertragungsnetze, zentrale Steuerung. Dieses

JULIA ENGELS, geb. 1994 in Aachen, ist Politikwissenschaftlerin und promoviert an der RWTH Aachen. Sie forscht zur internationalen Sicherheitsordnung und nuklearen Abschreckung.

1 Vgl. Stromausfall, [bkk.bund.de](https://www.bkk.bund.de), 31.1.2023.

2 Vgl. Massive russische Angriffe. 1,2 Millionen ukrainische Haushalte ohne Strom, [tagesschau.de](https://www.tagesschau.de), 24.1.2026.

Modell versprach Skaleneffekte, Stabilität, sinkende Kosten und war die Grundlage für den wirtschaftlichen Aufstieg zahlreicher Industriestaaten. Elektrizität wurde zum Motor industrieller Produktion, zum Garanten urbanen Lebens und zum Symbol technischen Fortschritts.

Doch je stärker ein System auf wenige zentrale Knotenpunkte angewiesen ist, desto mehr werden diese zu strategischen Zielen. Ein einzelnes Kraftwerk kann Millionen Menschen versorgen oder Millionen Menschen vom Strom abschneiden.

gen ermöglicht: industrielle Produktion, globale Kommunikation, massenhafte Mobilität. Gleichzeitig hat diese Infrastruktur eine neue Qualität von Abhängigkeit erzeugt. Die Stabilität des Alltags hängt heute mehr denn je von der Funktionsfähigkeit technischer Systeme ab.

Infrastruktur ist daher nie neutral. Wer Energie kontrolliert, kontrolliert zentrale Bedingungen gesellschaftlichen Lebens. Diese Einsicht ist keineswegs neu. Bereits im Zeitalter der Industrialisierung war Energiepolitik eng mit staatlicher Macht verbunden. Kohleförderung, Eisenbahnbau und Elektrifizierung waren immer auch politische Projekte.

Diese Logik hat sich im digitalen Zeitalter noch einmal verschärft: Rechenzentren, Kommunikationsnetze und Dateninfrastrukturen sind vollständig von stabiler Stromversorgung abhängig. Fällt sie aus, kommt die Industrie zum Stillstand und mit ihr die Informationsgesellschaft. Heute bemisst sich Sicherheit daher nicht mehr allein an militärischer Stärke oder territorialer Kontrolle, sondern zunehmend an der Fähigkeit, kritische Infrastrukturen funktionsfähig zu halten.⁴ Der Schutz solcher Infrastrukturen wird dadurch zu einer zentralen Aufgabe moderner Staaten.

Resilienz als politisches Konzept

Vor diesem Hintergrund wird zunehmend über Resilienz debattiert. Gemeint ist die Fähigkeit eines Systems, Störungen zu absorbieren und dennoch funktionsfähig zu bleiben.⁵ Dabei geht es nicht um Unverletzlichkeit, sondern um Anpassungsfähigkeit. Systeme gelten als resilient, wenn sie alternative Strukturen aktivieren, Ausfälle kompensieren und sich nach Krisen rasch reorganisieren können. Um resilient zu sein, dürfen Gesellschaften nicht

4 Vgl. Grundlagen und Rahmenbedingungen deutscher und internationaler Sicherheitspolitik, baks.bund.de, 4.1.2011.

5 Vgl. Resilienz. Lage der Cybersicherheit in den Dimensionen der Cybersicherheit, bsi.bund.de, März 2026.

»Fällt der Strom aus, gerät eine ganze Kette lebenswichtiger Funktionen ins Stocken.«

Dieser Logik folgt Russland im Krieg gegen die Ukraine: Kraftwerke, Umspannwerke und Übertragungsleitungen sind keine Kollateralschäden, sondern bewusst gewählte Ziele.

Die Wirkung solcher Angriffe erklärt sich aus der strukturellen Vernetzung fortschrittlicher Infrastrukturen. Stromausfälle betreffen Haushalte, sie legen Verkehrssysteme lahm, unterbrechen Kommunikationsnetze und beeinträchtigen medizinische Versorgung. Krankenhäuser verfügen zwar über Notstromaggregate, aber deren Kapazität ist begrenzt. Wasserversorgung und Abwasserentsorgung hängen vielfach von elektrischen Pumpen ab. Fällt der Strom aus, gerät eine ganze Kette lebenswichtiger Funktionen ins Stocken. Anfang Januar führte ein Brandanschlag zum längsten Stromausfall in der Berliner Nachkriegsgeschichte.³

Diese Kaskadeneffekte sind charakteristisch für hochkomplexe technische Systeme. Moderne Gesellschaften haben im Laufe des 20. Jahrhunderts eine Infrastruktur geschaffen, die enorme Leistun-

3 Vgl. Nach Stromausfall in Berlin: Diskussionen über Ausbau der kritischen Infrastruktur, deutschlandfunk.de, 8.1.2026.

allein auf Effizienz setzen, sondern zusätzlich auf Vorsorge. Einige Staaten haben dies frühzeitig erkannt: Russlands Nachbar Estland etwa investierte nach massiven Cyberangriffen im Jahr 2007 systematisch in digitale Sicherheitsarchitekturen und Notfallmechanismen.⁶ Dänemark verfolgt seit Jahren einen Ansatz, der auf Diversifizierung und Dezentralität setzt. Der hohe Anteil erneuerbarer Energien sowie die Einbindung lokaler Energiegenossenschaften haben dort ein System hervorgebracht, das weniger stark von einzelnen zentralen Anlagen abhängig ist.⁷ Im kriegsgeplagten Israel wiederum gehört der Schutz kritischer Infrastruktur seit 2002 zum sicherheitspolitischen Kernbestand. Folglich war Israel global einer der ersten Staaten mit einer Strategie zum Schutz der kritischen Infrastruktur. Angesichts permanenter Bedrohungslagen wurden dort früh Schutzkonzepte sowie schnelle Wiederherstellungsmechanismen konstruiert.⁸ Diese Beispiele veranschaulichen: Resilienz ist kein technischer Nebeneffekt, sondern das Ergebnis politischer Prioritäten und langfristiger Investitionen.

Energiewende und Verwundbarkeit

Deutschland befindet sich in dieser Hinsicht in einer Übergangsphase. Einerseits hat die Energiewende das hiesige Energiesystem bereits tiefgreifend verändert. Millionen Photovoltaikanlagen, Windparks und Biomassekraftwerke speisen inzwischen Strom ein. Der Anteil erneuerbarer Energien wächst langsam, aber kontinuierlich.⁹ Auf den ersten Blick scheint dies ein Schritt in Richtung Dezentralisierung zu sein. Andererseits werden Stromflüsse jedoch überregional ge-

steuert, gewinnen digitale Steuerungssysteme an Bedeutung und entstehen neue Abhängigkeiten. Auch die Elektrifizierung anderer Sektoren nimmt zu: Wärmepumpen ersetzen fossile Heizungen, Elektromobilität wächst an, digitale Dienstleistungen durchdringen nahezu alle Lebensbereiche. Strom wird damit noch stärker zum zentralen Energieträger moderner Gesellschaften.

Diese Entwicklung hat eine paradoxe Konsequenz. Während erneuerbare Energien strukturell mehr Dezentralität ermöglichen, wächst zugleich die Bedeutung stabiler Netze. Die Energiewende verändert also nicht nur die Energiequellen, sondern auch die Systemarchitektur.

»Dezentralität allein garantiert noch keine Sicherheit.«

Mit den neuen Chancen entstehen neue Risiken. Cyberangriffe auf Energieversorger etwa sind längst Teil geopolitischer Auseinandersetzungen.¹⁰ Digitale Steuerungssysteme ermöglichen also Effizienz, eröffnen aber auch neue Angriffspunkte. Hinzu kommen klimatische Risiken. Besonders Extremwetterereignisse wie Stürme, Hitzeperioden, Überschwemmungen können Leitungen beschädigen, die Kühlwasserzufuhr beeinträchtigen oder Netze überlasten. Die Klimakrise wirkt als Infrastrukturrisiko.¹¹

Verwundbarkeit entsteht somit nicht ausschließlich durch Krieg, sondern auch durch Umweltveränderungen und technologische Komplexität. Moderne Gesellschaften stehen einer Vielzahl möglicher Störungen gegenüber.

Dadurch gewinnt die Solarenergie zusätzlich an Bedeutung - als Instrument der Dekarbonisierung wie potenziell als Baustein infrastruktureller Resilienz.

6 Vgl. »Im Cyberspace hält immer jemand Ausschau nach deinen Schwächen«, srf.ch, 19.11.2022.

7 Vgl. Kathinka Burkhardt, Windkraft und Wärmewende. Was Dänemark in der Energiewende besser macht, energiewinde.orsted.de, 2.5.2022.

8 Vgl. Government of Israel, Special Resolution B/84, The responsibility for protecting computerized systems in the State of Israel, Jerusalem, 11.12.2002.

9 Vgl. Erneuerbare Stromerzeugung mit verhaltenem Wachstum, umweltbundesamt.de, 11.12.2025.

10 Vgl. Politik unterschätzt Dringlichkeit, bdi.eu, 6.1.2026.

11 Vgl. Sarah Steffen, So belastet der Klimawandel unsere Infrastruktur, dw.com, 30.7.2025.

Photovoltaikanlagen auf Dächern, kombiniert mit Batteriespeichern, ermöglichen lokale Versorgung und reduzieren Abhängigkeiten von zentralen Anlagen. Wo Stromerzeugung räumlich verteilt ist, wird ihre vollständige Lahmlegung schwieriger. Gleichzeitig eröffnet die Dezentralisierung neue Formen gesellschaftlicher Beteiligung. Bürgerinnen und Bürger werden zu Produzenten, Kommunen zu aktiven Gestaltern ihrer Energieversorgung.

Allerdings garantiert Dezentralität allein noch keine Sicherheit. Digitale Steuerungssysteme können manipuliert werden, lokale Netze bleiben anfällig für physische Schäden. Resilienz entsteht nicht automatisch durch Technologie, sondern durch kluge Systemarchitektur und politische Gestaltung.

Energieversorgung als Machtfrage

Der Blick auf die Ukraine zeigt, dass die Energieinfrastruktur nicht nur eine ökonomische, sondern auch eine humanitäre Bedeutung besitzt. Ohne Strom funktionieren Intensivstationen nicht, ohne Wärme sind Wohnungen im Winter unbewohnbar, ohne stabile Netze geraten soziale Dienste an ihre Grenzen. Der Schutz kritischer Infrastruktur wird damit grundlegend für eine freiheitliche Gesellschaft.¹² In der Energiepolitik muss daher stets Sicherheitspolitik mitgedacht werden. Investitionen in Netzausbau, Speichertechnologien sowie Cyberabwehr sind keine optionalen Modernisierungen, sondern die Voraussetzung gesellschaftlicher Stabilität.

Der Krieg gegen die Ukraine verdeutlicht, dass sich Macht im digitalen Zeitalter nicht einzig in Panzern oder Raketen ausdrückt. Er macht sichtbar, was in friedlichen Zeiten leicht übersehen wird: Moderne Gesellschaften beruhen auf hochkomplexen Infrastrukturen, die im Alltag nahezu unsichtbar bleiben. Strom-

netze, Kommunikationssysteme und Versorgungsketten funktionieren so zuverlässig, dass ihre Fragilität selten ins öffentliche Bewusstsein tritt. Erst wenn Transformatoren brennen, Leitungen zerstört werden oder ganze Regionen im Dunkeln liegen, wird deutlich, wie sehr das gesellschaftliche Leben von diesen technischen Systemen abhängt.

Für Europa heißt das: Der Schutz kritischer Infrastruktur darf nicht länger als technisches Randthema betrachtet werden, sondern gehört ins Zentrum sicherheitspolitischer Debatten.¹³ Resilienz bedeutet mehr als die Fähigkeit, Störungen kurzfristig zu überstehen. Sie verlangt langfristige Planung, institutionelle Vorbereitung und die Bereitschaft, gesellschaftliche Verwundbarkeit politisch ernst zu nehmen. Moderne Gesellschaften sind auf stabile Infrastrukturen angewiesen, und diese Stabilität entsteht nicht von selbst. Sie ist das Ergebnis politischer Entscheidungen, wirtschaftlicher Investitionen sowie gesellschaftlicher Prioritätensetzungen.

Die Angriffe auf die ukrainische Energieinfrastruktur erinnern uns daran, dass Energieversorgung längst zu einer Frage politischer Macht geworden ist.¹⁴ Resilienz ist im 21. Jahrhundert letztlich eine Voraussetzung politischer Selbstbehauptung. Sie entscheidet darüber, ob eine Gesellschaft auch unter Druck handlungsfähig bleibt - ob Krankenhäuser arbeiten, Kommunikationsnetze funktionieren und Wohnungen im Winter beheizt werden können.¹⁵ Im Ernstfall definiert sich die Stärke moderner Gesellschaften nicht ausschließlich an der Front, sondern darüber, ob ihre Infrastruktur standhält und ob das Licht weiter brennt. ◻

12 Vgl. Philip Banze und Ulf Buermeyer, Warum es der Politik schwerfällt, für gute Infrastruktur zu sorgen, bpb.de, 28.2.2025.

13 Vgl. Lisa Brüßler, Kritis-Dachgesetz verabschiedet. So will die Koalition den Schutz kritischer Infrastruktur verstärken, das-parlament.de, 30.1.2026.

14 Vgl. Yuriy Honcharenko und Yuri Mindyuk, Blackout in Kyjiw. Stromnetz im Visier, hss.de, 3.3.2026.

15 Vgl. Linda Roy, Resilienz ist Verteidigung und gehört ins Zentrum der Sicherheitspolitik, tuev-verband.de, 12.2.2026.