Bundesakademie
für Sicherheitspolitik

Arbeitspapier Sicherheitspolitik, Nr. 1/2026 28. Januar 2026

Bedingt resilient:
Was der Berliner Blackout Anfang 2026 für die deutsche Krisenvorsorge bedeutet

von Wolfgang Rudischhauser, Tobias Fella, Mateusz Łabuz und Matthias Schulze

Der mehrtägige Blackout mehrerer Stadtteile im Südwesten Berlins Anfang 2026 infolge eines Anschlags gegen eine Stromversorgungsleitung verdeutlicht dringenden Handlungsbedarf für Resilienz und Krisenvorsorge in Deutschland. Das gilt insbesondere, weil die Kritische Infrastruktur der Bundesrepublik, nicht erst seit dem russischen Angriff auf die Ukraine, häufiges Ziel hybrider Angriffe ist, und Ausfälle über unmittelbare Schäden für Bevölkerung und Wirtschaft hinaus auch zur Erosion von Vertrauen in das Funktionieren von Staat und Wirtschaft führen können. Der Staat ist auf allen Ebenen gefordert, Resilienz zu stärken und im Krisenfall Handlungsfähigkeit zu demonstrieren, glaubwürdig zu kommunizieren und Abhilfe aufzuzeigen. Neben der notwendigen Ausstattung der Behörden und Hilfsorganisationen erfordert dies auch Investitionen in ehrenamtliche Strukturen und zivilgesellschaftliches Engagement.

Der Anschlag auf eine unzureichend gesicherte Stromversorgungsleitung im Südwesten Berlins am 3. Januar 2026 führte zu einem mehrtägigen Blackout ganzer Stadtteile. Über 45.000 Haushalte blieben tagelang ohne Strom und Heizung; zu Beginn der Krise war auch der Mobilfunkempfang stark beeinträchtigt. Auch mehrere wichtige S-Bahnen- und Regionalzuglinien fuhren mangels Strom für die Stellwerke zeitweise nicht. Während Krankenhäuser auf ihre Notstromversorgung zugreifen mussten, konnte diese in Pflegeeinrichtungen erst mit einiger Verzögerung durch mobile Notstromaggregate sichergestellt werden. Teilweise musste die zur Unterstützung gerufene Bundeswehr die Aggregate mittels Tankwagen mit Treibstoff versorgen. Erst am 6. Januar war die Stromversorgung durch Notleitungen teilweise wiederhergestellt und schließlich am 9. Januar wieder stabil in Betrieb. Der Vorfall macht deutlich, dass es beim Schutz Kritischer Infrastruktur (KRITIS) nicht allein um die Abwehr von Angriffen geht, sondern um die Fähigkeit, trotz Störungen funktionsfähig zu bleiben und sich rasch zu erholen – also um echte Resilienz. In Deutschland herrscht dabei häufig ein falsches Verständnis darüber, was Resilienz eigentlich bedeutet. Sie wird oft mit Unverwundbarkeit oder der Fähigkeit verwechselt, Angriffe vollständig abzuwehren. Tatsächlich geht es jedoch darum, Störungen zu bewältigen, sich anzupassen und kritische Systeme schnell wieder funktionsfähig zu machen.

Vor diesem Hintergrund legte der mehrtägige Blackout in Berlin grundlegende Defizite in der Krisenvorsorge und der Resilienz Kritischer Infrastruktur in der Hauptstadt und mutmaßlich in Deutschland insgesamt offen. Fachleute warnen seit Jahren, dass KRITIS, wie Strom, Telekommunikation, Wasser, Gas und weitere Versorgungseinrichtungen in Deutschland nicht ausreichend gegen Sabotage und Eingriffe von außen geschützt ist. Während schnell ein Bekennerschreiben eines Absenders auftauchte, der sich als linksextreme Gruppe ausgab, blühten gleichzeitig Spekulationen, dass Formulierungen darin auf Übersetzungen aus dem Russischen und damit auf eine verdeckte Aktion Russlands hindeuten könnten. Der Generalbundesanwalt übernahm die Ermittlungen. Auch wenn die Spekulationen bisher unbestätigt geblieben sind, führte dies zu weiterer Verunsicherung. Wie groß die Verletzlichkeit insbesondere der Energieinfrastruktur ist, zeigt die Tatsache, dass es sich bereits um den dritten Vorfall in der Region Berlin mit schwerwiegenden Folgen innerhalb von zwei Jahren handelt. So führten Brandanschläge auf Stromleitungen im September 2025 zum Blackout eines ganzen Gewerbegebiets in

 | ISSN 2366-0805

Berlin-Adlershof und im März 2024 zur Abschaltung des Tesla-Werks im brandenburgischen Grünheide. Dass es jeweils mehrere Tage dauerte, die Stromversorgung über Ersatzleitungen wiederherzustellen, verdeutlicht zudem die weiterhin unzureichend vorhandenen Redundanzen und die mangelnde Netzresilienz. In Berlin verlaufen noch immer Teile der Hochspannungsleitungen oberirdisch – wobei der Trend zur umfassenden Erdung geht – und sind kaum gegen Fremdzugriffe geschützt. Erschwerend kommt hinzu, dass viele Informationen zur Kritischen Infrastruktur, teilweise Transparenzvorgaben folgend, öffentlich zugänglich sind. Die Verletzlichkeiten beschränken sich jedoch nicht auf Berlin und auch nicht allein auf die Energieversorgung. Seit Jahren verzeichnen die Behörden eine Zunahme von Angriffen auf die Verkehrsinfrastruktur. Kabeldiebstahl und Sabotage führten etwa 2023 und 2024 zu kurzzeitigen Ausfällen der Bahnstrecken Berlin-Hamburg und Bremen-Hamburg. Verschiedene Flughäfen mussten wegen Drohnensichtungen zeitweise gesperrt werden.

Zwar hatte das Bundeskabinett bereits im Herbst 2025 das sogenannte KRITIS-Dachgesetz beschlossen. Das Gesetz soll Betreiber und Versorger der Kritischen Infrastruktur in Deutschland zum besseren Schutz und zur Überwachung ihrer Einrichtungen gegen Fremdeingriffe verpflichten. Es sieht für Betreiber wesentlicher Sektoren wie Energie, Verkehr und Gesundheit umfassende Schutzmaßnahmen vor. Dazu zählen ein systematisches Risikomanagement, das Aufrechterhalten des Notbetriebs in Krisenlagen sowie die Planung von Verfahren, Ressourcen und Abläufen zur schnellen Wiederherstellung nach einer Störung – inklusive regelmäßiger Übungen. Bis Anfang 2026 wurde der Gesetzentwurf jedoch nicht vom Parlament verabschiedet. Das Bundesministerium des Innern kündigte infolge des Berliner Vorfalls eine Priorisierung an.

Ende Januar 2026 ist nun mit der zeitnahen Verabschiedung des KRITIS-Dachgesetzes zu rechnen. Als problematisch an dem Entwurf war schon zuvor insbesondere durch Sachverständige bei der Anhörung im Bundestag kritisiert worden, dass die geplanten Vorschriften häufig erst für Betreiber mit einer Versorgungszuständigkeit von über 500.000 Menschen griffen, wodurch viele regionale und kommunale Einrichtungen ausgenommen gewesen wären. Wie hoch dieser Schwellenwert ist, zeigt sich daran, dass er das Fünffache der rund 100.000 vom Berliner Blackout betroffenen Menschen beträgt. Der Vorfall bestätigte somit die Forderung, die Schwellenwerte zu überprüfen. Übertragen ließe sich diese Debatte auch auf die nationale Umsetzung der 2023 verabschiedeten EU-NIS2-Richtlinie zur Cybersicherheit – abermals vor allem im Hinblick auf Kommunen und Betreiber mit weniger als 500.000 Kunden. Medien berichteten jüngst, dass auf Drängen der Bundesländer in das KRITIS-Dachgesetz zumindest die Möglichkeit aufgenommen werde, dort jeweils selbst niedrigere Schwellenwerte anzusetzen – die dann allerdings nicht mehr bundesweit einheitlich wären. Ebenso sei den Berichten zufolge vorgesehen, Transparenzpflichten zur Offenlegung von Standort- oder Leistungsdaten zu überprüfen, da diese von fremden Nachrichtendiensten oder Extremisten zur Sabotageplanung missbraucht werden können.

Stärkung der Reaktionskapazitäten

Der Berliner Vorfall, aber auch andere Krisen wie das schwere Ahrtalhochwasser 2021, zeigen: Bei der Krisenwarnung und den Reaktionskapazitäten, nicht nur denen des Katastrophenschutzes, in Deutschland besteht dringender Handlungsbedarf. In beiden Fällen erreichten Warnungen, etwa durch Krisenapps wie „NINA“ oder „KATWARN”, die Betroffenen zu spät oder nur unzureichend. Hinzu kommt, dass Katastrophen- und Bevölkerungsschutz in Deutschland nach wie vor stark föderal organisiert sind. Selbst auf Länderebene verteilen sich die Verantwortlichkeiten häufig auf verschiedene Ressorts – in Berlin etwa auf die Senatsverwaltung für Inneres, die Feuerwehr, die Polizei sowie auf die einzelnen Bezirksämter der zwölf Stadtbezirke. Zwar existiert im Land Berlin seit 2020 ein Kompetenzzentrum für Bevölkerungsschutz und Krisenmanagement (KBK); dieses darf jedoch bisher nur planerisch und koordinierend tätig werden. Die operative Entscheidungskompetenz verbleibt bei den einzelnen Akteuren. Und zumindest zu Beginn der Krise blieb bisweilen unklar, wer für wofür zuständig ist. Berlin will dies nun rasch ändern und „Modellstadt“ für Krisenfestigkeit werden. Von den nach dem letzten Stromausfall vom Berliner Senat angekündigten 45 Katastrophenschutz-Leuchtturm-Einrichtungen, die in Krisen als Anlaufstelle zur Ersthilfe dienen sollen, ist bislang erst knapp ein Drittel einsatzbereit– wie der Berliner Rechnungshof in seiner deutlichen Kritik an den Krisenvorbereitungen kurz zuvor bemängelt hatte.

Auch deutschlandweit ist die Lage im Krisenmanagement weiterhin unbefriedigend. Die Bundesrepublik verfügt bislang nicht über ein nationales Krisenzentrum zur Koordination überregionaler Krisenreaktionen, wie es beispielsweise in Belgien seit 2018 existiert. Stattdessen ist im Koalitionsvertrag 2025 neben dem bereits eingerichteten Nationalen Sicherheitsrat die Einrichtung eines „Bund-Länder- und ressortübergreifenden Nationalen Krisenstabs" und eines „Nationalen Lagezentrums" vorgesehen, die zum einen 24/7 akutes Krisenmanagement betreiben und zum anderen ständig ein nationales Lagebild verfügbar haben sollen. Neben dem Technischen Hilfswerk (THW) kann die Bundeswehr laut Grundgesetz in besonderen Notlagen – und auf Anforderung – Hilfe leisten und per Amtshilfe zivile Kräfte wie Feuerwehr, Polizei und anerkannte Hilfsorganisationen unterstützen. Dies ist jedoch nur möglich, wenn militärische Ressourcen nicht im Kernauftrag der Bundeswehr, also der Landes- und Bündnisverteidigung, gebunden sind.

Geopolitischer Kontext: Hybride Angriffe gegen die Demokratie

Nicht funktionierende Krisenreaktion und unzureichende Notversorgungsstrukturen machen eine Gesellschaft anfällig für hybride Angriffe. Russland setzt im Rahmen seiner hybriden Kriegsführung – insbesondere seit dem Überfall auf die Ukraine 2022 – vermehrt sogenannte „aktive Maßnahmen", die physische Sabotage, Cyberangriffe und Desinformation verbinden, gegen westliche Gesellschaften ein. Ziel solcher hybriden Aktivitäten ist es, das Vertrauen der Bevölkerung in die Handlungsfähigkeit des Staates zu untergraben. Diese Maßnahmen setzen vor allem dort an, wo gesellschaftliche Spannungen, Misstrauen oder Versorgungsdefizite bereits existieren. Die Verletzlichkeit Kritischer Infrastruktur schafft eine doppelte Verwundbarkeit: Durch Sabotage lässt sich materieller und wirtschaftlicher Schaden anrichten, und zugleich kann dies die Wahrnehmung stärken, Staat und Wirtschaft könnten ihre grundlegenden Funktionen nicht mehr erfüllen – unabhängig davon, wer den Schaden verursacht hat. Unklarheiten bei der Identifikation der Urheber (zum Beispiel russische Sabotage vs. linksextremes Bekennerschreiben) sind ebenfalls Teil der hybriden Strategie. In der aktuellen Aufmerksamkeitsökonomie sehen sich Politiker und Politikerinnen oft zu vorschnellen Zuschreibungen veranlasst, was ungewollt selbst zu Verunsicherung und gesellschaftlicher Polarisierung beiträgt. In der angespannten Stimmung nach dem Stromausfall versuchten einige Akteure zudem, die Notlage der Berliner Bevölkerung zu instrumentalisieren. So titelte etwa die Berliner Zeitung am 5. Januar 2026: „*Während in Berlin das Licht ausgeht: 1.700 THW-Generatoren sichern Energie in der Ukraine*" – und bediente damit ein Narrativ, das auf Polarisierung abzielt.

Der Vorfall in Berlin sollte als Warnsignal und als Übung für den Ernstfall verstanden werden. Besonders kritisch wäre ein Szenario, in dem mehrere koordinierte Sabotageakte an verschiedenen Orten in Deutschland verübt werden, um die Reaktions- und Durchhaltefähigkeit der Bevölkerung und staatlicher Institutionen zu testen – etwa mit der gezielten Botschaft: „Wollt ihr wegen der Ukraine im Dunkeln sitzen und frieren? Seht her, eure Regierung hat Geld für den Schutz der Ukraine, aber nicht für euch". Deutschland ist aufgrund seiner geografischen Lage, seines Leistungspotenzials und seiner Rolle als europäische Führungsmacht ein Primärziel hybrider Aktivitäten, nicht zuletzt aufgrund seiner Bedeutung für die militärische Verlegefähigkeit der NATO nach Osten. Aktivitäten wie das Ausspähen von Logistikinfrastruktur, Drohnenflüge über Flughäfen und Kasernen sowie Sabotageakte an kriegsrelevanten Bahnverbindungen lassen sich daher auch als Vorbereitung auf künftige Konflikte deuten. Während die weltpolitische Krisenanfälligkeit ständig zunimmt und auch die interne Kohärenz der NATO zunehmend auf die Probe gestellt wird, bleiben die Krisenreaktions- und Notfallfähigkeiten Deutschlands und Europas jedoch absehbar unzureichend.

Eine technische Krise kann schnell zu einer Vertrauenskrise werden

Von entscheidender Bedeutung ist nicht nur, wie lange die technische Wiederherstellung der Stromversorgung oder anderer Kritischer Infrastruktur dauert, sondern auch, wie lange die Bevölkerung bereit ist, Störungen zu akzeptieren, ohne das Vertrauen in öffentliche Institutionen zu verlieren. In einer zunehmend digitalisierten Gesellschaft kann ein Strom- oder Internetausfall heute nicht nur Unannehmlichkeiten verursachen. Er kann den Verlust von Einkommen, Arbeitsmöglichkeiten, Informationszugang und grundlegenden Dienstleistungen bedeuten – und die Abhängigkeit davon wächst stetig. Dadurch werden langanhaltende Infrastrukturausfälle

zu einem äußerst wirksamen Faktor für politischen Druck und Destabilisierung – selbst ohne militärische Eskalation. Wenn der Staat – von der kommunalen bis zur nationalen Ebene – in einer solchen Situation Schwächen bei der Handlungsfähigkeit demonstriert, nicht glaubwürdig kommuniziert und keine klaren Abhilfemaßnahmen aufzeigt, kann sich eine technische Krise rasch zu einer Vertrauenskrise ausweiten. Aus dieser Perspektive sind Investitionen in die Resilienz der Infrastruktur zugleich Investitionen in die Resilienz der Demokratie. Denn das Gefühl von Sicherheit und Verlässlichkeit in der Gesellschaft bestimmt maßgeblich ihre Fähigkeit, unter Druck funktionsfähig zu bleiben. Die Folgen eines länger anhaltenden Stromausfalls treffen die Bevölkerung zudem ungleich. An Leib und Leben gefährdet sind besonders ältere Menschen und chronisch kranke Personen, die auf elektrische Geräte angewiesen sind. Darüber hinaus hängt der Lebensunterhalt einer noch weit größeren Gruppe von Menschen direkt davon ab, dass die digitale oder logistische Infrastruktur funktioniert. Unabhängig davon, welcher dieser Gruppen Menschen angehören, kann eine technische Krise rasch Existenzen bedrohen. Enttäuschung und das Gefühl, vom Staat im Stich gelassen zu werden, können im Zusammenspiel damit wiederum Nährboden für radikalisierende Narrative und gezielte Desinformation bieten.

Gesellschaftliche Resilienz fördern

Ein entscheidender Faktor, der die Auswirkungen einer solchen Krise abfedern kann, ist die gesellschaftliche Solidarität – also das Maß an Vertrauen, die Stärke sozialer Netzwerke und die Fähigkeit zur Selbstorganisation auf lokaler Ebene. Gemeinschaften mit engen nachbarschaftlichen Bindungen, aktiven zivilgesellschaftlichen Organisationen und einer Kultur gegenseitiger Hilfe sind besser in der Lage, staatliche Untätigkeit oder Verzögerungen zumindest teilweise auszugleichen, Panik zu begrenzen und grundlegende soziale Funktionen auch bei langanhaltenden Störungen der Infrastruktur aufrechtzuerhalten. Dies gelingt in ländlichen Regionen und kleineren Kommunen tendenziell leichter als in anonymisierten und teils stark von Zu- Wegzug geprägten Großstädten. Fluktuation steht oft nachhaltigem bürgerschaftlichem Engagement entgegen. Ein Problem können auch Finanzierungslücken bei ehrenamtlichen Strukturen sein, was wiederum das bürgerschaftliche Engagement schwächen kann. Auch deshalb sollten Politik und Behörden sich für den Aufbau von sozialen Basisstrukturen interessieren. Gerade der Berliner Vorfall zeigt: Kommunen und Länder müssen – unterstützt durch Bundesprogramme – bestehende ehrenamtliche Strukturen gezielt ausbauen, indem sie Ausbildung, Ausrüstung und Nachhaltigkeitskonzepte (wie zum Beispiel Nachfolgeregelungen) fördern, statt sie neu von Null zu schaffen.

Ein zentraler Aspekt der sozialen Resilienz ist ihre kognitive Dimension, die über technische, infrastrukturelle und physische Faktoren hinausgeht. Sie betrifft psychologische Mechanismen und die Fähigkeit einer Gesellschaft, auf psychologischen Druck zu reagieren. Gegner demokratischer Staaten nutzen gezielt solchen kognitiven Druck, um gesellschaftliche Wahrnehmungen und Reaktionen zu beeinflussen. China beschreibt diese Methoden in seinen strategischen Konzepten, während Russland weiterhin auf Instrumente der sogenannten „reflexiven Kontrolle“ zurückgreift, die darauf zielt, Gegner zu Handlungen bewegen, die im Interesse Moskaus liegen. Ereignisse wie der Stromausfall in Berlin bieten ideale Angriffsflächen im Informationsraum, um Verunsicherung zu vertiefen und gewünschte Narrative zu verstärken. In solchen Situationen wird die Fähigkeit der Behörden, schnell, klar und konsistent zu kommunizieren, zu einem zentralen Faktor für das Krisenmanagement. Dazu gehören proaktive Kommunikationsstrategien ebenso, wie ein ausgeprägtes Situationsbewusstsein, das auf kontinuierlicher Informationsanalyse, Lagebewertung und Austausch basiert.

Bei einem großflächigen Stromausfall hängt die Wirksamkeit öffentlicher Kommunikation jedoch auch von der physischen Verfügbarkeit der Informationskanäle ab. Wenn Strom, Internet und Mobilfunk nur eingeschränkt verfügbar sind, wird ein erheblicher Teil der Bevölkerung vom digitalen Informationsfluss abgeschnitten. Gelingt es dem Staat nicht, Kommunikationswege zu diversifizieren, entsteht schnell ein Vakuum, das von Gerüchten, Fehlinformation und Desinformation gefüllt wird. Echte Informationsresilienz in Krisenzeiten erfordert daher nicht nur strategische Vorbereitung und abgestimmte Botschaften, sondern auch deren physische Zugänglichkeit für die Bevölkerung. Klassische Kanäle wie UKW-Radio, lokale Notfallinformationsstellen, Sirenen, Megafone und akustische Warnsignale, mobile Lautsprecherwagen sowie Satellitenfunk können dabei entscheidend sein, um sicherzustellen, dass der Staat selbst in Phasen technischer Ausfälle als sichtbarer und glaubwürdiger Akteur im öffentlichen Raum präsent bleibt.

Was sollte Deutschland aus dem Berliner Blackout lernen?

Zunächst ist der Staat insgesamt bei der Schaffung von Resilienz im Sinne von Widerstands- und Anpassungsfähigkeit des Systems aus Staat, Wirtschaft und Gesellschaft gefordert. Auch wenn die Bürgerinnen und Bürger mit Eigenschutz- und Versorgungsmaßnahmen die erste Linie der Resilienz bilden, kann der oder die Einzelne – wie sich jüngst in Berlin zeigte – nicht alles auffangen. Ein effektiver Katastrophenschutz ist nur möglich, wenn Staat, Wirtschaft, Zivilgesellschaft sowie Bürgerinnen und Bürger gemeinsam handeln. Finnlands Strategie etwa verbindet Behörden, Unternehmen und Gesellschaft in einem „All-Gefahren"-Ansatz, der sowohl zivile als auch militärische Bedrohungen abdeckt. Wichtige Elemente für Deutschland sind Notfallplanung, Kontinuitätsmanagement, regelmäßige Übungen und eine Echtzeit-Lageüberwachung durch ein Regierungslagezentrum. Persönliche Krisenvorsorge ist ebenso essenziell wie ausreichende finanzielle Mittel für Katastrophenschutz, Feuerwehr, Polizei und auf Bundesebene das THW. Auch die Bundeswehr sollte so ausgestattet sein, dass es in nationalen Krisenszenarien nicht zu einer Ressourcenkonkurrenz kommt, der die Erfüllung ihres Kernauftrags gefährdet. Zentral für Krisenvorsorge und -reaktion ist dabei, die Bevölkerung einzubeziehen. Schweden bereitet seine Bürgerinnen und Bürger bereits seit Jahrzehnten praktisch und mental auf größere Krisen vor. Seit 2018 (und erneut 2024) erhält die Bevölkerung eine Vorsorgebroschüre mit Empfehlungen unter dem Titel „Im Falle von Krisen oder Krieg". Zwar gibt es in Deutschland seit 2013 ebenfalls eine – regelmäßig aktualisierte – Vorsorgebroschüre des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe; diese wird aber nicht aktiv allen Haushalten zugestellt.

Der Staat – also Bund, Länder und Kommunen – sollte vor allem zur Gefahrenabwehr Abhängigkeiten reduzieren, etwa durch Gasspeicher und die Stärkung dezentraler Energieversorgung. Er muss resiliente Netzstrukturen für Daten und Kommunikation bereitstellen sowie Betreiber zu *Back-up*-Systemen verpflichten. Vorsorglicher Bevölkerungsschutz in Friedenszeiten sollte außerdem den Aufbau und die Wartung von Schutzräumen und medizinischer Reserven beinhalten. Fatalerweise wurde in Deutschland erst vor wenigen Jahren auf Druck der Mobilfunkbetreiber die Verpflichtung abgeschafft, Mobilfunkmasten mit Notstromkapazitäten für mindestens acht Stunden zu versorgen. Auch Kommunen und kommunale IT-Betreiber sollten das bekannte Kompendium von Cybersicherheitsmaßnahmen („IT-Grundschutz") verinnerlichen und regelmäßige Übungen durchführen. Zugleich muss bei der weiteren Umsetzung der Energiewende die Sicherheitsplanung dringend stärker einbezogen werden – etwa durch die Schaffung autonomer Versorgungszellen (Balkonsolar, dezentrale Energiespeicher, Windkraft, Nord-Süd-Stromkorridore, Wabenstruktur der Netze), um Ausfälle besser regional begrenzen zu können. Andere Nationen wie etwa Finnland, Japan und Südkorea führen regelmäßig groß angelegte Katastrophenschutzübungen durch, um Selbstwirksamkeit und gegenseitige zivile Fürsorge der Bevölkerung zu trainieren. Solche Übungen ermöglichen es zugleich Behörden, ihre Kommunikationsprozesse mit der Bevölkerung unter Notbedingungen zu testen und Kommunikationsdesaster wie jüngst in Berlin zu vermeiden. In Deutschland findet dagegen nur alle drei Jahre eine bundesländerübergreifende Katastrophenübung (LÜKEX) statt, die sich vor allem auf Stabsebene abspielt. Ohne eingeübte Praxis bleiben selbst die besten Katastrophenschutzkonzepte theoretisch.

Schließlich gilt: Wenn die Bevölkerung einen Staat wahrnimmt, der grundsätzliche öffentliche Güter effektiv bereitstellt und zur nationalen Sicherheit angemessen beiträgt, wird sie auch eher bereit sein, Engpässe zu akzeptieren. Festzuhalten bleibt allerdings auch: Selbst bessere Vorsorge garantiert keinen hundertprozentigen Schutz. Moderne Infrastruktur ist weit verzweigt und zugleich fragil; mit fortschreitender Digitalisierung entstehen zusätzliche Abhängigkeiten und Verwundbarkeiten. Resilienz bedeutet in diesem Zusammenhang immer auch, das Eintreten von Schäden zu antizipieren – um dann schnellstmöglich zur Funktionsfähigkeit zurückzukehren. Es geht also um eine angemessene Vorbereitung, wobei Resilienz in diesem Fall stark mit ausreichender Vorsorge („*Preparedness*") korreliert. Gleichzeitig betreffen diese *Preparedness* und Resilienz das gesamte System der Funktionsweise des Staates und seiner Bürgerinnen und Bürger, darunter zahlreiche infrastrukturelle, logistische, organisatorische, soziale und politische Aspekte. Ohne ein Bündel abgestimmter Maßnahmen ist die nächste Krise vorprogrammiert. Benjamin Franklin formulierte das einst treffend: *„By failing to prepare, you are preparing to fail"*.

***Wolfgang Rudischhauser** ist Non-Resident Fellow; **Dr. Tobias Fella**, **Dr. Mateusz Łabuz** und **Dr. Matthias Schulze** sind Wissenschaftliche Mitarbeiter am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). Die Autoren geben ihre persönliche Meinung wieder.*