JETZT ENDLICH HANDELN! BEVÖLKERUNG SCHÜTZEN, UNSERE INFRASTRUKTUREN KRISENFEST MACHEN

Fraktionsvorstandsbeschluss vom 19. Januar 2026

Zehntausende Menschen und Tausende Betriebe waren zum Jahresbeginn 2026 in Berlin bei eiskaltem Winterwetter tagelang ohne Strom. Dieser Sabotageangriff hat uns drastisch vor Augen geführt: Fällt der Strom aus, bleiben auch die Heizungen kalt und die Wasserversorgung kommt zum Erliegen, da Pumpen und Steuerungen versagen; die Mobilfunknetze brechen zusammen. Das ist verheerend und nicht der erste Angriff auf die Stromversorgung. Wir weisen seit Jahren auf die Verletzlichkeit der kritischen Infrastrukturen (KRITIS) als Lebensadern unserer Gesellschaft hin.

In solchen Situationen muss zunächst schnellstmöglich und unbürokratisch geholfen werden. Die Berliner Zivilgesellschaft hat hier große Solidarität gezeigt, die Feuerwehr, das THW, die Hilfsorganisationen und Kirchen mit Ehrenamtler*innen haben enormes Engagement und Know-how gezeigt. Ganz anders aber Innenminister Dobrindt, der auf Bundesebene zuständig ist und von dem nichts zu sehen war. Für alle sind die massiven Versäumnisse beim Schutz von kritischer Infrastruktur und Bevölkerung sichtbar, die er als Bundesinnenminister direkt zu verantworten hat. Der Katastrophenschutz und die Abwehr von Angriffen auf die kritische Infrastruktur müssen eine Gemeinschaftsaufgabe der Länder und des Bundes sein.

Es braucht endlich eine echte Sicherheitsoffensive, umfassende Prävention und einen besser koordinierten Bevölkerungs- und Katastrophenschutz. Bereits vor Monaten haben wir eine Gesamtstrategie skizziert: mehr Ressourcen, bessere Ausstattung, klare Strukturen und zeitgemäße gesetzliche Grundlagen.

Bundeskanzler Merz hatte in seiner Regierungserklärung vom 16. Oktober 2025 einen umfassenden Aktionsplan zur effektiven Bekämpfung hybrider Angriffe versprochen. Davon ist in der Realität und im Alltag der Menschen noch nichts angekommen. Wer etwas zur Chefsache erklärt, steht in der Verantwortung, mehr als Ankündigungen zu liefern. Nicht einmal die EU-Vorgaben der NIS-2- und der CER-Richtlinie zum KRITIS-Schutz wurden bisher einheitlich umgesetzt. Der Gesetzentwurf von Innenminister Dobrindt für ein „KRITIS-Dachgesetz“ wurde im Bundestag von Sachverständigen als massiv unzulänglich verrissen. Die Kritik, auch aus der Wirtschaft, wächst täglich. Dennoch verlängert Dobrindt das jahrelange Zaudern des Innenministeriums beim Schutz kritischer Infrastruktur. Weder er noch der Berliner Senat haben Lehren daraus gezogen, dass es im September 2025 bereits einen Anschlag auf das Berliner Stromnetz gegeben hat. Auch am 3. Januar hatte der Regierende Bürgermeister von Berlin erst mal anderes zu tun, als Hilfe zu koordinieren, und hat darüber auch noch die Unwahrheit gesagt. Gerade in einer Krise braucht es aber vollen Fokus und eine hohe Glaubwürdigkeit.

Wir setzen uns für eine sicherheitspolitisch informierte Energiepolitik ein, die den Schutz vor hybriden Angriffen, die technologische Souveränität und die Klimaneutralität ins Zentrum stellt. Erneuerbare Energien sind „Freiheitsenergien“ und „Sicherheitsenergien“ zugleich: Sie reduzieren nicht nur CO_2-Emissionen, sondern machen ein Land im hybriden und

militärischen Ernstfall resilient. Denn eine dezentrale Energieinfrastruktur ist schwerer zu sabotieren und zu zerstören.

Großflächige Stromausfälle durch Sabotageaktionen, Attacken auf Bahngleise, ein Totalausfall des Bürgeramts, weil Kommunalverwaltungen gehackt werden – all das kann alle und überall treffen. Mit gezielten Drohnenüberflügen werden Sicherheitsbereiche sowie Infrastruktur ausspioniert und Verunsicherung geschürt, mit IT-Angriffen Chaos verursacht und massiver volkswirtschaftlicher Schaden angerichtet. Terroristische Anschläge, Sabotage und andere hybride Angriffe autoritärer Staaten, allen voran Russlands, sollen unsere Gesellschaft verunsichern und unsere Demokratie zersetzen. Dem müssen wir uns entschieden entgegenstellen. Dabei tragen auch die Unternehmen Verantwortung und haben für Resilienz ihrer Infrastruktur sowie ihrer Lieferketten zu sorgen.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) stellt zu Recht heraus: In einer wehrhaften Demokratie ist individuelle und kollektive Resilienz ein Akt der Selbstbehauptung. Nach dem verheerenden Anschlag in Berlin müssen die Verantwortlichen in Bundesinnenministerium und Kanzleramt jetzt endlich aufwachen. Wir brauchen eine Sicherheitsoffensive und eine gemeinsame Kraftanstrengung, um als Gesellschaft widerstands- und im Krisenfall schnell handlungsfähig zu sein.

Die wichtigsten Eckpunkte für eine Sicherheitsoffensive für Deutschland:

- **Kritische Infrastruktur schützen – einheitlich und ohne Ausnahmen:** Strom, Wasser, Gesundheit, Kommunikation, öffentliche Verwaltung – was unsere Gesellschaft am Laufen hält, braucht verlässlichen Schutz **– mit einem umfassenden KRITIS-Dachgesetz können wir unsere Infrastruktur härten.** Der Entwurf der Bundesregierung wird den aktuellen Bedrohungen nicht gerecht. Deutschland muss insbesondere durch das Schaffen von einheitlichen Mindeststandards, Risikoanalysen und ein Störungsmonitoring widerstandsfähiger gegen Krisen und Angriffe werden.

- **Zivilschutz krisenfest machen:** Die Bundesgesetze für den Zivilschutz sind jahrzehntealt und passen nicht mehr auf die neuen Herausforderungen. Das Zivilschutz- und Katastrophenhilfegesetz sowie die Vorsorge- und Sicherstellungsgesetze müssen dringend reformiert werden. Feuerwehr, THW und die Hilfsorganisationen brauchen mit Blick auf ihre unverzichtbare Rolle im Bevölkerungsschutz mehr Ressourcen, bessere Ausstattung und klare Strukturen. Mit dem Sondervermögen haben wir es ermöglicht, über den Bund viel Geld auch für den Bevölkerungsschutz einzusetzen. **Jeder Euro in die kommunale Infrastruktur ist ein Beitrag für mehr Resilienz.** Die Bundesregierung muss gegenüber den Ländern einfordern, die zur Verfügung gestellten Mittel des Sondervermögens schnellstens zur Stärkung des Katastrophenschutzes zu verwenden und bei der **Modernisierung von 2.000 Feuerwehrhäusern pro Jahr** unterstützen. Es braucht **eine deutliche personelle Stärkung des THWs und mehr Ortsverbände im Osten Deutschlands.** Wer sich freiwillig für unsere Gesellschaft im Bevölkerungsschutz einsetzen möchte, verdient bessere Informationen und mehr Anerkennung für das Engagement.

- **Selbstwirksamkeit stärken:** Erforderlich ist **klare Kommunikation** zum richtigen Verhalten für den Krisenfall statt ängstliches Vermeiden von Debatten. Es braucht dringend eine Informationsoffensive der Bundesregierung, die die Haushalte zur Vorsorge für Krisen und auch auf Stromausfälle animiert. Denn eine resiliente Gesellschaft beginnt beim resilienten Individuum. Ein Plan und klare Kommunikation machen Mut und führen zum Erfolg.

- **Grundgesetz modernisieren – Institutionen stärken:** Das **föderale Sicherheitsgefüge** insgesamt gehört auf den Prüfstand und muss an die Herausforderungen unserer Zeit angepasst werden. Wichtige Aufgaben wie die effektive Abwehr von Drohnen, der Schutz von KRITIS sowie der Bevölkerungs- und Katastrophenschutz könnten als **Gemeinschaftsaufgabe** von Bund und Ländern besser erfüllt werden. Gerade im Katastrophenschutz muss der Bund endlich Verantwortung übernehmen. Gleichzeitig benötigt es eine stärkere finanzielle Handlungsfähigkeit der Kommunen für flächendeckende Prävention und die Härtung von öffentlicher Infrastruktur.

- **Für Aufklärung und effektive Strafverfolgung sorgen:** Die Hintergründe von Anschlägen und Sabotageaktionen müssen engagiert ermittelt und die Öffentlichkeit muss seriös und transparent informiert werden. Es ist gut, dass der Generalbundesanwalt nun die Ermittlungen beim Anschlag auf das Berliner Stromnetz übernommen hat. Es war ebenso gut, dass die Bundesregierung Ende 2025 die Verantwortung Russlands für Cyberangriffe und Wahlbeeinflussungen zur Bundestagswahl 2025 ausdrücklich benannt hat. Solche Transparenz ist notwendig, um die Resilienz unserer Demokratie zu stärken. **Zudem muss das Strafrecht im Bereich Spionage und Sabotage umfassend modernisiert werden, um neuen Angriffsformen wirksam zu begegnen.**

- **Lagebild statt Blindflug:** Wir brauchen ein zentrales und laufend aktualisiertes **Gesamtlagebild zu hybriden Bedrohungen in Deutschland**. Erst mit einem klaren Lagebild haben Bund und Länder eine gemeinsame Grundlage für Entscheidungen, sowohl in der Gefahrenabwehr als auch als Grundlage für weitere gesetzgeberische Schritte. Zielführend im Einsatz für die bestmöglichen Szenarien wäre die Einrichtung eines **Zentrums für strategische Vorausschau**, das Risiken für unsere Sicherheit in allen Bereichen früher erkennt.

- **Härtung der Netzinfrastruktur – Redundanzen schaffen:** Angesichts gezielter Sabotage und hybrider Bedrohungen muss sichergestellt werden, dass Ausfallsicherheit auch bei mutwilligen Zerstörungen, die über einen technischen Defekt hinausgehen, gegeben ist. Beim Neu- und Umbau von Umspannwerken
und Netzknoten muss eine **räumliche Trennung der Redundanzleitungen** erfolgen, um Schwachstellen zu vermeiden, wie dies bei der Kabelbrücke in Berlin der Fall gewesen sein könnte, bei der auch das Ausweichkabel mit zerstört wurde. Die technische Infrastruktur für den „Inselbetrieb“ (Microgrids) muss ertüchtigt werden, um lokale Versorgung auch bei Ausfall des Übertragungsnetzes zu ermöglichen.

- **Transparenz und Informationssicherheit bei kritischer Energieinfrastruktur:** Transparenz ist ein Kernwert der Energiewende, darf aber nicht zur Blaupause für Sabotage werden. Wir fordern einen gestaffelten Zugang zu Netzinformationen: Während grobe Planungsdaten für die Bürgerbeteiligung öffentlich bleiben, müssen sensible Geodaten, detaillierte Schaltpläne und exakte GPS-Koordinaten von Transformatorenstationen in digitalen Systemen geschützt und nur für Personen mit berechtigtem Interesse zugänglich sein.

- **IT-Sicherheit erhöhen**: Wir müssen digitale Abhängigkeiten erfassen, massiv reduzieren und die Souveränität Deutschlands und Europas steigern. Zentrale Einrichtungen wie das Bundesamt für Sicherheit (BSI) in der Informationstechnik müssen gestärkt und es dem BSI als Zentralstelle per Grundgesetzänderung endlich ermöglicht werden, die Länder bei der Abwehr schwerwiegender Gefahren durch IT-Angriffe zu unterstützen.

- **Aufbau von Souveränitätstechnologien:** Energiesicherheit braucht eine gesicherte Lieferkette. Deshalb fordern wir die konsequente Einführung von Resilienz-Ausschreibungen. Bei der

Vergabe von Großprojekten müssen europäische Wertschöpfung, IT-Sicherheit und Lieferkettensicherheit schwerer gewichtet werden als der reine Anschaffungspreis. Der Aufbau einer strategischen Produktion von Windanlagen, Wärmepumpen und Batterietechnologien, aber auch Stromnetzkomponenten wie Kabeln in Deutschland und Europa ist eine notwendige Investition in unsere nationale Sicherheit.