D-01 Dringlichkeitsantrag: Für ein krisenfestes Land: Kritische Infrastruktur schützen und den Bevölkerungsschutz stärken

Gremium:	Bundesvorstand
Beschlussdatum:	13.10.2022
Tagesordnungspunkt:	V Verschiedenes

Antragstext

Der russische Angriffskrieg auf die Ukraine stellt einen historischen Einschnitt in die europäische Friedensordnung dar. Der Krieg geht mit unermesslichem menschlichem Leid einher.
Auch zivile Infrastrukturen sind massiven Attacken ausgesetzt. Die aktuellen und schrecklichen Bilder haben uns noch einmal vor Augen geführt, wie verletzlich eine moderne
und vernetzte Gesellschaft ist. Gleichzeitig müssen auch wir feststellen, dass es zunehmend
Angriffe auf unsere Kritischen Infrastrukturen (KRITIS) gibt. Diese beschäftigen uns seit Jahren, nehmen aber derzeit in ihrer Intensität deutlich zu: Bereits im Frühjahr wurden ungewöhnlich viele Angriffe auf die IT-Systeme von Unternehmen aus der Windkraftbranche
verzeichnet. Ende September wurden mit gewaltigen Sprengstoffanschlägen die Gas-Pipelines
von Nord Stream 1 und Nord Stream 2 in der See vor Bornholm massiv beschädigt. Anfang
Oktober wurde mit zwei synchronisierten und professionellen Anschlägen auf Kommunikationskabel der Deutschen Bahn der Zugverkehr in Norddeutschland zeitweise
großflächig lahmgelegt. All diese Ereignisse stehen in einem zeitlichen Zusammenhang. Sie
haben das Ziel, unsere Gesellschaft in einer von Krisen gekennzeichneten Zeit weiter zu

verunsichern. Sie stellen in ihren Auswirkungen eine neue Qualität dar und nutzen sowohl
digitale als auch physische Schwachstellen der Kritischen Infrastruktur aus. Die entstandenen Schäden zeigen uns, dass auch bereits verhältnismäßig einfache Störaktionen,
wie die Durchtrennung der Kabel bei den Anschlägen auf die Bahn, eine große Wirkung entfalten können.

Kritische Infrastrukturen sind die Lebensader einer jeden Gesellschaft. Dazu zählen z.B. die
Energieversorgung, die Kommunikation, der Verkehrsbereich oder das Gesundheitswesen. Der
Schutz Kritischer Infrastrukturen ist ein zentraler Baustein für ein krisenfestes Land. Die

Wehrhaftigkeit unserer Gesellschaft beweist sich auch auf diesem Gebiet. Leider zeigen die
Attacken auch, dass es um den Schutz von Kritischen Infrastrukturen in Deutschland trotz
jahrelanger Diskussionen, beispielsweise nach weitreichenden Angriffen auf den

Deutschen
Bundestag, noch immer nicht besonders gut bestellt ist. Zentrale Risiken wurden viel zu lange sträflich vernachlässigt und sicherheitspolitisch falsche Prioritäten gesetzt. Dabei haben auch Naturkatastrophen oder andere Schadensereignisse immer wieder gezeigt, dass wir unzureichend auf Ausfälle einzelner Systeme vorbereitet sind.

Auf die Notwendigkeit, diese Themen proaktiv anzugehen und gesellschaftliche Resilienz zu erhöhen haben wir als grüne in den vergangenen Jahren immer wieder hingewiesen. Die derzeitige Debatte um die mangelhafte Krisenfähigkeit unserer Gesellschaft und die Erkenntnisse, die wir im Zuge der jüngsten Angriffe gewinnen konnten, machen deutlich, wie notwendig es ist, die vielen, von uns Grünen hierzu im Koalitionsvertrag verankerten Projekte entschlossen umzusetzen. Besonders mit Blick auf Kritische Infrastrukturen erleben wir eine Verschränkung von innerer und äußerer Sicherheit. Deshalb ist der Schutz von Kritischer Infrastruktur eine Herausforderung, die es innen- wie außenpolitisch zu bewältigen gilt. Gerade jetzt ist es notwendig, dass Politik und Sicherheitsbehörden kurzfristig Maßnahmen ergreifen, um Kritische Infrastrukturen zu schützen. Die Polizeien von Bund und Ländern müssen wichtige Einrichtungen und z.B. Kontenpunkte von Kommunikation verstärkt in den Blick nehmen. Dazu sind sie mit den entsprechenden Ressourcen auszustatten.
Die Spionageabwehr muss neu aufgestellt und ggf. gestärkt werden. Und wir brauchen neue Strukturen zur Erkennung und Abwehr hybrider Bedrohungen. Die Zusammenarbeit in Einrichtungen wie dem Nationalen Cyberabwehrzentrum muss nach klaren gesetzlichen Vorgaben erfolgen. Aktive Cyberabwehr im Rahmen von Hackbacks schließen wir aus.

Jetzt ist es höchste Zeit zu handeln und entschieden kurz- und langfristig in unseren Schutz und in gesamtstaatliche Resilienz zu investieren. Dazu gehört, dass wir dort, wo es notwendig ist, redundante Rückfallebenen schaffen, damit bei Ausfällen oder Störungen nicht gleich ganze Systeme ausfallen. Hierzu können z.B. getrennte Kommunikationsverbindungen gehören. Digitale und physische Komponenten müssen viel stärker zusammen gedacht werden.
Heute sind Anforderungen an Kritische Infrastrukturen vor allem im Rahmen der IT-Sicherheitsgesetzgebung formuliert. Diese ist jedoch nach Meinung vieler Expert*innen nicht ausreichend. Anforderungen an den physischen Schutz geraten viel zu oft aus dem Blick.
Gleichzeitig sind Schwellenwerte teils so hoch angesetzt, dass selbst große Betreiber von kritischen Einrichtungen durch das Raster fallen. Diese Lücken müssen dringend geschlossen

werden. Einen ganzheitlichen Rahmen zum Schutz wichtiger Infrastruktur soll ein „KRITIS-Dachgesetz“ bilden, das alle kritischen Infrastrukturen abdeckt und ein Gesamtlagebild zu erstellen erlaubt. Das Gesetz ist heute dringender denn je und muss umgehend auf den Weg gebracht werden.

Die Zusammenarbeit von den unterschiedlichen Behörden, die mit dem Schutz Kritischer Infrastrukturen betraut sind, muss ebenfalls dringend verbessert werden. Hierzu zählt insbesondere eine bessere Vernetzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die Zusammenarbeit der Behörden und Einrichtungen muss auf klare Rechtsgrundlagen gestellt werden und insbesondere die Arbeit des BSI unabhängiger von politischer Weisung sein, damit es seinen Aufgaben nachkommen kann. Hierzu zählen insbesondere das schnelle und konsequente Schließen von Sicherheitslücken in IT-Systemen und ein wirksames Schwachstellenmanagement. Eine kohärente digitale Strategie zum Schutz von IT-Systemen darf nicht akzeptieren, dass Sicherheitslücken nicht geschlossen werden. Ebenso sind dafür mehr und höhere Standards in Bezug auf IT-Sicherheit notwendig. Auch die Polizeibehörden und Nachrichtendienste müssen hier einen Paradigmenwechsel einleiten und stehen in gesamtgesellschaftlicher Verantwortung.

Die kürzlich vom Bundesministerium des Inneren und für Heimat (BMI) vorgelegte Cybersicherheitsstrategie wird diesem Anspruch bisher nicht gerecht. Daher kommt es nun im besonderen Maße darauf an, dass die Nationale Sicherheitsstrategie, die derzeit unter Federführung des Auswärtigen Amtes erarbeitet wird, sowohl diese Aspekte berücksichtigt, als auch Cyberaußenpolitik.

Insgesamt müssen wir weg von einer noch immer rein reaktiven IT-Sicherheitspolitik, die diejenigen, die Opfer eines Angriffs geworden sind, noch bestraft. Was es braucht sind proaktive Strategien, die diejenigen, die von sich aus in gute IT-Sicherheit investieren wollen, hierbei unterstützen – auch finanziell.

Neben echten Investitionen zur Krisenprävention müssen wir auch die verbesserte Bewältigung von Schadenslagen in den Blick nehmen. Eine besondere Bedeutung kommt hierbei dem Bevölkerungsschutz, also dem Zivil- und Katastrophenschutz, zu. Eine gute Vorbereitung hilft im Ernstfall, Schäden abzuwenden oder zu verringern.

Die vergangenen Jahre haben wiederholt gezeigt, dass bei großflächigen oder besonderen Schadenslagen die Fähigkeiten der Länder an Grenzen stoßen können. Ein Beispiel hierfür sind die Hochwasserkatastrophe im vergangenen Jahr, aber auch die Brände im Sommer dieses Jahres. Dieser Umstand ist für den Ausfall von Kritischen Infrastrukturen von besonderer Bedeutung. Eine gute und länderübergreifende Koordination von Hilfsmaßnahmen kann dabei helfen, Schäden abzuwenden. Deutschland verfügt mit seinem guten Netz an Behörden und Organisationen sowie rund 1,7 Millionen Freiwilligen im Bevölkerungsschutz im gesamten Land über große Ressourcen und viel Expertise. Damit Hilfe im Ernstfall schnellstmöglich zur Verfügung steht, müssen Lageinformationen und Fähigkeiten besser erfasst und koordiniert werden. Die Neuausrichtung des BBK sowie die Einrichtung einer Zentralstelle sind hierfür von besonderem Gewicht. Das im BBK existierende Gemeinsame Lagezentrum (GMLZ) ist entsprechend auszubauen. Das gemeinsame Kompetenzzentrum Bevölkerungsschutz (GeKoB) muss so ausgebaut werden, dass es aktuelle Informationen zum Bevölkerungsschutz aus den Ländern zusammenführt und so in einer Krise die Bewältigung aktiv unterstützen kann. Dafür sind die gesetzlichen und finanziellen Voraussetzungen jetzt zu schaffen.

Eine nachhaltige Stärkung des BBK ist auch notwendig, damit das Amt seine Aufgabe als oberste Zivilschutzbehörde besser wahrnehmen kann. Aktuell kann das BBK dieser Aufgabe kaum gerecht werden. Der Schutz der Zivilbevölkerung im Spannungs- und Verteidigungsfall gehört zu den obersten Pflichten eines jeden Staates. Die militärische und zivile Verteidigung steht in einem direkten Zusammenhang. Sie müssen als Gesamtverteidigung begriffen werden.
Die sicherheitspolitische Debatte hat diesen Umstand bisher noch nicht ausreichend berücksichtigt und vor allem wurden bisher nicht genügend finanzielle Mittel zur Verfügung gestellt. Dabei macht sich jeder in den Zivilschutz investierte Euro bezahlt und steht auch für andere Gefahrenlagen zur Verfügung: Die Warnung der Bevölkerung durch den Aufbau eines umfassendes „Warnmixes“ mit Cell-Broadcasting, Apps oder Sirenen. Die Unterbringung und Versorgung von geflüchteten Menschen. Der Aufbau mit Versorgungskapazitäten von Trinkwasser oder Notstrom. All diese Vorhaltungen helfen uns auch bei Naturkatastrophen oder

anderen
Schadensereignissen.

Die vielleicht wichtigste Lehre aus den großen Katastrophen der vergangenen Jahre ist, dass
Krisenszenarien regelmäßig über Ressort- und Ländergrenzen hinweg geübt werden müssen. Nur
so kann eine bessere Verzahnung gelingen und Investitionen Früchte tragen. Dabei müssen
Übungen von der Bundesebene bis in die Kommunen reichen und praktische Fähigkeiten
aufgreifen. Nur so können Fehler erkannt und Fähigkeitslücken geschlossen werden.

Die wichtigste Säule im Bevölkerungsschutz stellen die zahlreichen freiwilligen Helfer*innen
der Hilfsorganisationen, der Feuerwehren und des Technischen Hilfswerks (THW) dar. Ihnen
gilt unser Dank und unsere Anerkennung. Wir müssen dieses ehrenamtliche Engagement weiter
pflegen und fördern. Im Koalitionsvertrag sind hierzu zahlreiche Maßnahmen vorgesehen, die
nun mit Nachdruck vom BMI umgesetzt werden müssen. Hierzu zählt ein Ehrenamtskonzept oder
die Helfer*innengleichstellung. Wir müssen auch die digitale Kompetenz der Freiwilligen

stärker in den Bevölkerungsschutz einbringen. Der Aufbau eines „Cyberhilfswerkes“ beim THW
ist ein wichtiges Element, das wir in der Ampelkoalition bereits angestoßen haben. Das
„Cyberhilfswerk“ muss nun zügig aufgebaut und zusammen mit den Freiwilligen stetig
weiterentwickelt werden. Zu den möglichen Aufgaben könnten beispielsweise Hilfeleistungen
beim Zusammenbruch von IT-Systemen oder der Kommunikation gehören. Das digitale Ehrenamt
wollen wir weiter stärken.

Neben den Menschen, die freiwillig in den Blaulichtorganisationen engagiert sind, müssen wir
die Selbsthilfefähigkeit der Bevölkerung stärken. Das Auftreten multipler Krisen führt bei
vielen Menschen zu Verunsicherung. Eine sachliche Auseinandersetzung kann Ängste abbauen und
die Souveränität der Menschen steigern. Gleichzeitig stärkt sie das Gefühl für gemeinsame
Handlungsfähigkeit und Verantwortung. Die Vermittlung von grundlegenden
Selbsthilfefähigkeiten muss stärker Einzug in Bildungseinrichtungen und Arbeitsstätten finden.

Bedrohungslagen und Katastrophen machen nicht an Ländergrenzen halt. Daher müssen wir den
Bevölkerungsschutz noch stärker europäisch denken und Instrumente, wie das europäische
Katastrophenschutzverfahren sowie die europäische Katastrophenschutzreserve „rescEU“,

stärken. Sie sind Ausdruck gelebter europäischer Solidarität. Deutschland hat die Ukraine frühzeitig mit Nothilfemaßnahmen unterstützt und z.B. medizinisches Material, Ausrüstung oder Fahrzeuge geliefert. Auch werden Menschen mit Kriegsverletzungen in Deutschland behandelt. Das BSI hat bei der Analyse und Abwehr von IT-Angriffen unterstützt. Dieses Engagement müssen wir fortführen und wenn nötig stärken. Aber auch Deutschland kann auf die Hilfe unserer europäischen Freund*innen angewiesen sein. Dies wurde beispielsweise im Zuge des jüngsten Waldbrandes im Harz deutlich, bei dem wir vielfältige Unterstützung, unter anderem durch Löschflugzeige aus Italien, erfahren haben.

Die Zusammenarbeit im Bevölkerungsschutz müssen wir auch auf den Schutz von Kritischen Infrastrukturen übertragen. Egal ob das Strom- und Gasnetz, Telekommunikationsnetze und Unterseekabel oder länderübergreifende Verkehrswege sind. Sie alle sind gemeinsame zivile europäische Infrastruktur, die wir gemeinsam schützen müssen. Angriffe hierauf müssen geächtet werden. Gerade die Zunahme von hybriden Gefahren und das Verschwimmen der Grenzen von privaten und staatlichen Akteur*innen machen eine noch intensivere Zusammenarbeit notwendig. Ländern wie Russland muss Europa und die internationale Staatengemeinschaft glaubhaft und entschiedenen entgegentreten, wenn sie die Integrität dieser Systeme verletzten.

Begründung der Dringlichkeit

Die Serie an Störaktionen hat sich weiter vorgesetzt und hat mit den synchronisierten Anschlägen auf Kommunikationsverbindungen der Deutschen Bahn eine vorläufigen Höhepunkt im Inland gefunden. Dadurch ist auch die Debatte erneut entbrannt. Der Vorfall am 08. Oktober 2022 fand nach dem Antragsschluss statt.