

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

Gremium: Bundesvorstand
Beschlussdatum: 13.10.2022
Tagesordnungspunkt: V Verschiedenes

Antragstext

- 1 Der russische Angriffskrieg auf die Ukraine stellt einen historischen Einschnitt in die
2 europäische Friedensordnung dar. Der Krieg geht mit unermesslichem menschlichem Leid einher.
3 Auch zivile Infrastrukturen sind massiven Attacken ausgesetzt. Die aktuellen und
4 schrecklichen Bilder haben uns noch einmal vor Augen geführt, wie verletzlich eine moderne
5 und vernetzte Gesellschaft ist. Gleichzeitig müssen auch wir feststellen, dass es zunehmend
6 Angriffe auf unsere Kritischen Infrastrukturen (KRITIS) gibt. Diese beschäftigen uns seit
7 Jahren, nehmen aber derzeit in ihrer Intensität deutlich zu: Bereits im Frühjahr wurden
8 ungewöhnlich viele Angriffe auf die IT-Systeme von Unternehmen aus der Windkraftbranche
9 verzeichnet. Ende September wurden mit gewaltigen Sprengstoffanschlägen die Gas-Pipelines
10 von Nord Stream 1 und Nord Stream 2 in der See vor Bornholm massiv beschädigt. Anfang
11 Oktober wurde mit zwei synchronisierten und professionellen Anschlägen auf
12 Kommunikationskabel der Deutschen Bahn der Zugverkehr in Norddeutschland zeitweise
13 großflächig lahmgelegt. All diese Ereignisse stehen in einem zeitlichen Zusammenhang. Sie
14 haben das Ziel, unsere Gesellschaft in einer von Krisen gekennzeichneten Zeit weiter zu
15 verunsichern. Sie stellen in ihren Auswirkungen eine neue Qualität dar und nutzen sowohl
16 digitale als auch physische Schwachstellen der Kritischen Infrastruktur aus. Die
17 entstandenen Schäden zeigen uns, dass auch bereits verhältnismäßig einfache Störaktionen,
18 wie die Durchtrennung der Kabel bei den Anschlägen auf die Bahn, eine große Wirkung
19 entfalten können.
- 20 Kritische Infrastrukturen sind die Lebensader einer jeden Gesellschaft. Dazu zählen z.B. die
21 Energieversorgung, die Kommunikation, der Verkehrsbereich oder das Gesundheitswesen. Der
22 Schutz Kritischer Infrastrukturen ist ein zentraler Baustein für ein krisenfestes Land. Die
23 Wehrhaftigkeit unserer Gesellschaft beweist sich auch auf diesem Gebiet. Leider zeigen die
24 Attacken auch, dass es um den Schutz von Kritischen Infrastrukturen in Deutschland trotz
25 jahrelanger Diskussionen, beispielsweise nach weitreichenden Angriffen auf den Deutschen
26 Bundestag, noch immer nicht besonders gut bestellt ist. Zentrale Risiken wurden viel zu
27 lange sträflich vernachlässigt und sicherheitspolitisch falsche Prioritäten gesetzt. Dabei
28 haben auch Naturkatastrophen oder andere Schadensereignisse immer wieder gezeigt, dass wir
29 unzureichend auf Ausfälle einzelner Systeme vorbereitet sind.
- 30 Auf die Notwendigkeit, diese Themen proaktiv anzugehen und gesellschaftliche Resilienz zu
31 erhöhen haben wir als grüne in den vergangenen Jahren immer wieder hingewiesen. Die
32 derzeitige Debatte um die mangelhafte Krisenfähigkeit unserer Gesellschaft und die
33 Erkenntnisse, die wir im Zuge der jüngsten Angriffe gewinnen konnten, machen deutlich, wie
34 notwendig es ist, die vielen, von uns Grünen hierzu im Koalitionsvertrag verankerten
35 Projekte entschlossen umzusetzen. Besonders mit Blick auf Kritische Infrastrukturen erleben

36 wir eine Verschränkung von innerer und äußerer Sicherheit. Deshalb ist der Schutz von
37 Kritischer Infrastruktur eine Herausforderung, die es innen- wie außenpolitisch zu
38 bewältigen gilt. Gerade jetzt ist es notwendig, dass Politik und Sicherheitsbehörden
39 kurzfristig Maßnahmen ergreifen, um Kritische Infrastrukturen zu schützen. Die Polizeien von
40 Bund und Ländern müssen wichtige Einrichtungen und z.B. Kontaktpunkte von Kommunikation
41 verstärkt in den Blick nehmen. Dazu sind sie mit den entsprechenden Ressourcen auszustatten.
42 Die Spionageabwehr muss neu aufgestellt und ggf. gestärkt werden. Und wir brauchen neue
43 Strukturen zur Erkennung und Abwehr hybrider Bedrohungen. Die Zusammenarbeit in
44 Einrichtungen wie dem Nationalen Cyberabwehrzentrum muss nach klaren gesetzlichen Vorgaben
45 erfolgen. Aktive Cyberabwehr im Rahmen von Hackbacks schließen wir aus.

46 Jetzt ist es höchste Zeit zu handeln und entschieden kurz- und langfristig in unseren Schutz
47 und in gesamtstaatliche Resilienz zu investieren. Dazu gehört, dass wir dort, wo es
48 notwendig ist, redundante Rückfallebenen schaffen, damit bei Ausfällen oder Störungen nicht
49 gleich ganze Systeme ausfallen. Hierzu können z.B. getrennte Kommunikationsverbindungen
50 gehören. Digitale und physische Komponenten müssen viel stärker zusammen gedacht werden.
51 Heute sind Anforderungen an Kritische Infrastrukturen vor allem im Rahmen der IT-
52 Sicherheitsgesetzgebung formuliert. Diese ist jedoch nach Meinung vieler Expert*innen nicht
53 ausreichend. Anforderungen an den physischen Schutz geraten viel zu oft aus dem Blick.
54 Gleichzeitig sind Schwellenwerte teils so hoch angesetzt, dass selbst große Betreiber von
55 kritischen Einrichtungen durch das Raster fallen. Diese Lücken müssen dringend geschlossen
56 werden. Einen ganzheitlichen Rahmen zum Schutz wichtiger Infrastruktur soll ein „KRITIS-
57 Dachgesetz“ bilden, das alle kritischen Infrastrukturen abdeckt und ein Gesamtlayoutbild zu
58 erstellen erlaubt. Das Gesetz ist heute dringender denn je und muss umgehend auf den Weg
59 gebracht werden.

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

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

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

82 Neben echten Investitionen zur Krisenprävention müssen wir auch die verbesserte Bewältigung
83 von Schadenslagen in den Blick nehmen. Eine besondere Bedeutung kommt hierbei dem

84 Bevölkerungsschutz, also dem Zivil- und Katastrophenschutz, zu. Eine gute Vorbereitung hilft
85 im Ernstfall, Schäden abzuwenden oder zu verringern.

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

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

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

119 Die wichtigste Säule im Bevölkerungsschutz stellen die zahlreichen freiwilligen Helfer*innen
120 der Hilfsorganisationen, der Feuerwehren und des Technischen Hilfswerks (THW) dar. Ihnen
121 gilt unser Dank und unsere Anerkennung. Wir müssen dieses ehrenamtliche Engagement weiter
122 pflegen und fördern. Im Koalitionsvertrag sind hierzu zahlreiche Maßnahmen vorgesehen, die
123 nun mit Nachdruck vom BMI umgesetzt werden müssen. Hierzu zählt ein Ehrenamtskonzept oder
124 die Helfer*innengleichstellung. Wir müssen auch die digitale Kompetenz der Freiwilligen
125 stärker in den Bevölkerungsschutz einbringen. Der Aufbau eines „Cyberhilfswerkes“ beim THW
126 ist ein wichtiges Element, das wir in der Ampelkoalition bereits angestoßen haben. Das
127 „Cyberhilfswerk“ muss nun zügig aufgebaut und zusammen mit den Freiwilligen stetig
128 weiterentwickelt werden. Zu den möglichen Aufgaben könnten beispielsweise Hilfeleistungen
129 beim Zusammenbruch von IT-Systemen oder der Kommunikation gehören. Das digitale Ehrenamt
130 wollen wir weiter stärken.

131 Neben den Menschen, die freiwillig in den Blaulichtorganisationen engagiert sind, müssen wir
132 die Selbsthilfefähigkeit der Bevölkerung stärken. Das Auftreten multipler Krisen führt bei

133 vielen Menschen zu Verunsicherung. Eine sachliche Auseinandersetzung kann Ängste abbauen und
134 die Souveränität der Menschen steigern. Gleichzeitig stärkt sie das Gefühl für gemeinsame
135 Handlungsfähigkeit und Verantwortung. Die Vermittlung von grundlegenden
136 Selbsthilfefähigkeiten muss stärker Einzug in Bildungseinrichtungen und Arbeitsstätten
137 finden.

138 Bedrohungslagen und Katastrophen machen nicht an Ländergrenzen halt. Daher müssen wir den
139 Bevölkerungsschutz noch stärker europäisch denken und Instrumente, wie das europäische
140 Katastrophenschutzverfahren sowie die europäische Katastrophenschutzreserve „rescEU“,
141 stärken. Sie sind Ausdruck gelebter europäischer Solidarität. Deutschland hat die Ukraine
142 frühzeitig mit Nothilfemaßnahmen unterstützt und z.B. medizinisches Material, Ausrüstung
143 oder Fahrzeuge geliefert. Auch werden Menschen mit Kriegsverletzungen in Deutschland
144 behandelt. Das BSI hat bei der Analyse und Abwehr von IT-Angriffen unterstützt. Dieses
145 Engagement müssen wir fortführen und wenn nötig stärken. Aber auch Deutschland kann auf die
146 Hilfe unserer europäischen Freund*innen angewiesen sein. Dies wurde beispielsweise im Zuge
147 des jüngsten Waldbrandes im Harz deutlich, bei dem wir vielfältige Unterstützung, unter
148 anderem durch Löschflugzeuge aus Italien, erfahren haben.

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

Begründung der Dringlichkeit

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