

**Beschluss** Für ein krisenfestes Land: Kritische Infrastruktur schützen und den Bevölkerungsschutz stärken

Gremium: Bundesdelegiertenkonferenz  
Beschlussdatum: 16.10.2022  
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  
3 Leid einher.  
4 Auch zivile Infrastrukturen sind massiven Attacken ausgesetzt. Die aktuellen und  
5 schrecklichen Bilder haben uns noch einmal vor Augen geführt, wie verletzlich eine  
6 moderne  
7 und vernetzte Gesellschaft ist. Gleichzeitig müssen auch wir feststellen, dass es  
8 zunehmend  
9 Angriffe auf unsere Kritischen Infrastrukturen (KRITIS) gibt. Diese beschäftigen uns seit  
10 Jahren, nehmen aber derzeit in ihrer Intensität deutlich zu: Bereits im Frühjahr wurden  
11 ungewöhnlich viele Angriffe auf die IT-Systeme von Unternehmen aus der  
12 Windkraftbranche  
13 verzeichnet. Ende September wurden mit gewaltigen Sprengstoffanschlägen die Gas-  
14 Pipelines  
15 von Nord Stream 1 und Nord Stream 2 in der See vor Bornholm massiv beschädigt.  
16 Anfang  
17 Oktober wurde mit zwei synchronisierten und professionellen Anschlägen auf  
18 Kommunikationskabel der Deutschen Bahn der Zugverkehr in Norddeutschland  
19 zeitweise  
20 großflächig lahmgelegt. All diese Ereignisse stehen in einem zeitlichen Zusammenhang.  
21 Sie  
22 haben das Ziel, unsere Gesellschaft in einer von Krisen gekennzeichneten Zeit weiter zu  
23 verunsichern. Sie stellen in ihren Auswirkungen eine neue Qualität dar und nutzen  
24 sowohl  
25 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  
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. Knotenpunkte 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  
57 „KRITIS-  
58 Dachgesetz“ bilden, das alle kritischen Infrastrukturen abdeckt und ein Gesamtlagebild  
59 zu  
60 erstellen erlaubt. Das Gesetz ist heute dringender denn je und muss umgehend auf den  
61 Weg  
62 gebracht werden.

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

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

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

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

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

101 Eine nachhaltige Stärkung des BBK ist auch notwendig, damit das Amt seine Aufgabe  
102 als  
103 oberste Zivilschutzbehörde besser wahrnehmen kann. Aktuell kann das BBK dieser  
104 Aufgabe kaum  
105 gerecht werden. Der Schutz der Zivilbevölkerung im Spannungs- und Verteidigungsfall  
106 gehört  
107 zu den obersten Pflichten eines jeden Staates. Die militärische und zivile Verteidigung  
108 steht in einem direkten Zusammenhang. Sie müssen als Gesamtverteidigung begriffen  
109 werden.  
110 Die sicherheitspolitische Debatte hat diesen Umstand bisher noch nicht ausreichend  
111 berücksichtigt und vor allem wurden bisher nicht genügend finanzielle Mittel zur  
112 Verfügung  
113 gestellt. Dabei macht sich jeder in den Zivilschutz investierte Euro bezahlt und steht  
114 auch  
115 für andere Gefahrenlagen zur Verfügung: Die Warnung der Bevölkerung durch den  
116 Aufbau eines  
117 umfassendes „Warnmixes“ mit Cell-Broadcasting, Apps oder Sirenen. Die Unterbringung  
118 und  
119 Versorgung von geflüchteten Menschen. Der Aufbau mit Versorgungskapazitäten von  
120 Trinkwasser  
121 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,  
115 dass  
116 Krisenszenarien regelmäßig über Ressort- und Ländergrenzen hinweg geübt werden  
117 müssen. Nur  
118 so kann eine bessere Verzahnung gelingen und Investitionen Früchte tragen. Dabei  
119 müssen  
120 Übungen von der Bundesebene bis in die Kommunen reichen und praktische  
121 Fähigkeiten  
122 aufgreifen. Nur so können Fehler erkannt und Fähigkeitslücken geschlossen werden.  
123 Die wichtigste Säule im Bevölkerungsschutz stellen die zahlreichen freiwilligen  
124 Helfer\*innen  
125 der Hilfsorganisationen, der Feuerwehren und des Technischen Hilfswerks (THW) dar.  
126 Ihnen  
127 gilt unser Dank und unsere Anerkennung. Wir müssen dieses ehrenamtliche  
128 Engagement weiter  
129 pflegen und fördern. Im Koalitionsvertrag sind hierzu zahlreiche Maßnahmen  
130 vorgesehen, die  
131 nun mit Nachdruck vom BMI umgesetzt werden müssen. Hierzu zählt ein  
132 Ehrenamtskonzept oder  
133 die Helfer\*innengleichstellung. Wir müssen auch die digitale Kompetenz der Freiwilligen  
134 stärker in den Bevölkerungsschutz einbringen. Der Aufbau eines „Cyberhilfswerkes“  
135 beim THW  
136 ist ein wichtiges Element, das wir in der Ampelkoalition bereits angestoßen haben. Das  
137 „Cyberhilfswerk“ muss nun zügig aufgebaut und zusammen mit den Freiwilligen stetig  
138 weiterentwickelt werden. Zu den möglichen Aufgaben könnten beispielsweise  
139 Hilfeleistungen  
140 beim Zusammenbruch von IT-Systemen oder der Kommunikation gehören. Das digitale  
141 Ehrenamt  
142 wollen wir weiter stärken.  
143 Neben den Menschen, die freiwillig in den Blaulichtorganisationen engagiert sind,  
144 müssen wir  
145 die Selbsthilfefähigkeit der Bevölkerung stärken. Das Auftreten multipler Krisen führt  
146 bei  
147 vielen Menschen zu Verunsicherung. Eine sachliche Auseinandersetzung kann Ängste  
148 abbauen und  
149 die Souveränität der Menschen steigern. Gleichzeitig stärkt sie das Gefühl für  
150 gemeinsame  
151 Handlungsfähigkeit und Verantwortung. Die Vermittlung von grundlegenden  
152 Selbsthilfefähigkeiten muss stärker Einzug in Bildungseinrichtungen und Arbeitsstätten  
153 finden.  
154 Bedrohungslagen und Katastrophen machen nicht an Ländergrenzen halt. Daher  
155 müssen wir den  
156 Bevölkerungsschutz noch stärker europäisch denken und Instrumente, wie das  
157 europäische  
158 Katastrophenschutzverfahren sowie die europäische Katastrophenschutzreserve  
159 „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.