

Beschluss des Bundesvorstands der CDU Deutschlands

Berlin, 20. Oktober 2025

**Deutschland sicherer und widerstandsfähiger machen -
hybride Bedrohungen und Angriffe koordiniert und wirksam abwehren**

Viele Menschen in Deutschland machen sich Sorgen um ihre Sicherheit. Drohnen über Kasernen und Flughäfen, Sabotage an Bahnschienen und Stromnetzen, Cyberattacken auf Behörden und Krankenhäuser, gekappte Unterseekabel in der Ostsee, sogenannte Wegwerfagenten, die uns ausspionieren, als Nachrichten getarnte Propaganda oder Social-Media-Krieger, die als angebliche Influencer die öffentliche Meinung manipulieren: Die hybriden Angriffe, die wir in wachsender Zahl erleben, sind keine Zwischenfälle oder gar Zufälle. Sie zielen auf unsere Freiheit und Sicherheit. Sie zielen auf Demokratie, Wohlstand und Wirtschaft, auf den Zusammenhalt in unserem Land und unsere Art zu leben. Diese Angriffe gelten uns allen. Man will uns Angst machen und unser Vertrauen in den Staat und unsere freiheitliche Demokratie untergraben.

Wir befinden uns nicht im Krieg, aber unsere Freiheit, unser Frieden und unsere Sicherheit sind bedroht. An dieser Erkenntnis führt kein Weg vorbei. Und sie wirft die Frage auf: Wie gut sind wir vor hybriden Angriffen geschützt? Die ehrliche Antwort lautet: Wir müssen mehr tun, und wir werden mehr tun. Denn Stärke sichert Freiheit und Frieden. Schwäche hingegen lädt ein, unsere Widerstandskraft zu testen.

Unser Staat hat die Pflicht, die Menschen in Deutschland zu schützen und dafür Sorge zu tragen, dass sie in Freiheit und Sicherheit leben können.

Was Aggressoren anrichten können, sehen wir in der Ukraine – und immer öfter auch bei uns. Wir wissen: Innere und äußere Sicherheit lassen sich nicht mehr voneinander trennen. Gegen unbekannte Drohnen müssen Polizei und Bundeswehr zügig vorgehen können, besser zusammenwirken und sich gegenseitig helfen dürfen. Neben notwendigen Investitionen in die Bundeswehr ist es ebenso entscheidend, Bevölkerungsschutz und Zivilverteidigungsfähigkeit zu stärken.

Deshalb ist es ein Meilenstein, dass im neu geschaffenen Nationalen Sicherheitsrat (NSR) Wissen und Entscheidungsbedarfe zusammengeführt werden. Der NSR arbeitet an der Schnittstelle von innerer, äußerer, wirtschaftlicher und digitaler Sicherheit. Er bündelt relevante Erkenntnisse und bewertet sie, leistet strategische Vorausschau und Planung, widmet sich der Krisenprävention und ist ein Instrument der schnellen Reaktionsfähigkeit.

33 Wir begrüßen, dass sich der NSR in seiner ersten Sitzung schwerpunktmäßig mit hybriden
34 Bedrohungen beschäftigen wird und hierzu einen ressortübergreifenden Aktionsplan auf den
35 Weg bringt.

36 Wir wissen: Hybride Angreifer wollen immer auch testen, wie sehr wir bereit sind, uns zu
37 verteidigen und unser Land zu schützen. Wir sind bereit, alles zu tun, was nötig ist. Sicherheit
38 ist nicht nur Abwehr, sie ist auch Ausdruck von Stärke, von Vertrauen in die eigenen
39 Fähigkeiten. Deutschland muss wehrhaft bleiben, widerstandsfähiger werden und schneller
40 reagieren können.

41 Bund, Länder und Gemeinden müssen gemeinsam entschlossen handeln. Wir brauchen eine
42 moderne Ausstattung, bessere und schnellere Abwehrfähigkeiten, angepasste
43 Sicherheitsstrukturen, klar geregelte Zuständigkeiten, rechtssichere Eingriffsbefugnisse – und
44 ein gemeinsames, vom NSR erstelltes Lagebild, das ständig aktualisiert wird.

45 Die CDU ist seit jeher die Partei der inneren und der äußeren Sicherheit. Auf uns kann man sich
46 verlassen – auch und gerade jetzt im Kampf gegen unsichtbare Angreifer und jede Form
47 hybrider Gefahren. Wir Christdemokraten werden weiterhin alles tun, damit unser Land durch
48 eine besonnene, entschlossene und vorausschauende Politik eine sichere Zukunft hat.

49 **Gefahren aus dem Cyberraum abwehren**

50 Hybride Angreifer agieren auch im Cyberraum, weil sie die Urheberschaft ihrer Attacken im
51 Netz gut tarnen und verbergen können. Einige staatliche Akteure nutzen dabei auch kriminelle
52 und „haktivistische“ Gruppen, um die Herkunft des Angriffs zu verschleiern. Zahl,
53 Komplexität und Schwere von Cyberattacken wachsen beständig und sind alles andere als
54 harmlos. Sie treffen das Nervensystem unseres Landes. Wir müssen uns besser vor ihnen
55 schützen, technologische Führungsfähigkeit sichern und die staatliche Handlungsfähigkeit in
56 der digitalen Sphäre weiter stärken. Denn Cybersicherheit ist nicht statisch. Das Schutzniveau
57 heute garantiert keine erfolgreiche Abwehr der Angriffe von morgen.

58 Um auf diese dynamischen Entwicklungen angemessen reagieren zu können, müssen wir
59 unsere Schlagkraft fortwährend weiter erhöhen. Dabei ist entscheidend, dass unsere
60 Sicherheitsbehörden bei der Cybersicherheit mit den notwendigen Befugnissen, Fachpersonal
61 und moderner Infrastruktur ausgestattet werden.

62 Das Bundesamt für Sicherheit in der Informationstechnik (BSI) muss in enger Abstimmung mit
63 den Ländern zu einer Zentralstelle für Fragen der Informations- und Cybersicherheit
64 ausgebaut werden. So bekommt Deutschlands Cybersicherheitsarchitektur neben dem
65 Bundesamt für Verfassungsschutz und dem Bundeskriminalamt eine starke dritte Säule. Das

66 Nationale Cyber-Abwehrzentrum muss so weiterentwickelt werden, dass es im
67 Zusammenspiel mit dem NSR in komplexen Schadenslagen, wie etwa bei einem Angriff auf ein
68 Satellitennetzwerk, bundesweit eine Abwehr von Gefahren und Angriffen koordinieren kann.

69 Der Cyber- und Informationsraum (CIR) spielt eine wichtige Rolle für die Handlungsfähigkeit
70 der Bundeswehr in der digitalen Welt und zum Schutz unseres Landes vor digitalen
71 Bedrohungen. Für diese Aufgaben der nationalen Sicherheit braucht es das große Know-how
72 ziviler und militärischer Cyberexperten. Dafür muss die Cyber-Reserve weiter gestärkt werden.

73 Die stärkere gemeinsame Ausrichtung auf den CIR muss auch ein Schwerpunkt bei den
74 Nachrichtendiensten sein, auch durch die Schaffung einer neuen spezialisierten technischen
75 Zentralstelle unter Einbeziehung der Zentralen Stelle für Informationstechnik im
76 Sicherheitsbereich (ZITiS).

77 Es kommt jetzt darauf an, gemeinsam mit den Ländern die rechtlichen, organisatorischen und
78 technischen Voraussetzungen für eine starke aktive Cyberabwehr des Bundes zu schaffen.
79 Cyberangriffe müssen besser aufgeklärt und unterbunden werden können. Die zivilen und
80 militärischen Fähigkeiten zur Cyberabwehr müssen besser verzahnt, und es müssen
81 regelmäßige gemeinsame Cyberübungen der Bundes-, der Landes- und der kommunalen
82 Ebene vorgenommen werden.

83 Wir setzen uns dafür ein, beim BSI ein zentrales KI-Kompetenzzentrum für Cybersicherheit
84 einzurichten. Angreifer nutzen zunehmend KI-gestützte Verfahren zur automatisierten
85 Erkennung von Schwachstellen und zur Manipulation kritischer Systeme. Gleichzeitig bietet KI
86 bessere Chancen, Angriffe frühzeitig zu erkennen, zu analysieren und abzuwehren.
87 Deutschland benötigt daher eine nationale Einrichtung, die Forschung, Entwicklung und
88 operative Anwendung von KI in der Cyberabwehr strategisch bündelt und steuert.

89 **Bevölkerungsschutz stärken, kritische Infrastrukturen widerstandsfähiger machen**

90 Es gibt zahlreiche Beispiele, die belegen: Andere Staaten, vor allem autoritär regierte und
91 sogenannte Systemrivalen, greifen uns hybrid an und gefährden die Sicherheit der
92 Bevölkerung. Das heißt für uns: Deutschland muss spätestens bis zum Ende dieses Jahrzehnts
93 nicht nur verteidigungs-, sondern auch zivilschutzfähig sein.

94 Der Bevölkerungsschutz muss sich immer wieder auf veränderte Bedrohungen einstellen.
95 Dafür steht das Gemeinsame Kompetenzzentrum Bevölkerungsschutz. Auf dieser
96 Kooperationsplattform werden die Kräfte des gesamten Bevölkerungsschutzes in Bund,
97 Ländern, Kommunen und Hilfsorganisationen gebündelt. Mehr Zusammenarbeit für mehr
98 Schutz!

99 Mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) verfügt Deutschland
100 zudem über ein zentrales Organisationselement für die zivile Sicherheit. Dieses muss finanziell
101 und personell weiter so gestärkt werden, dass der Bevölkerungsschutz in einem integrativen
102 Netzwerk aller Akteure effektiv zusammenwirken kann. Mit einem „Pakt für den
103 Bevölkerungsschutz“ zwischen Bund und Ländern werden nachhaltige Investitionen in die
104 Ausstattung sichergestellt, insbesondere bei Unterbringung, Fahrzeugen und IT-Infrastruktur.

105 Für den Spannungs- oder Verteidigungsfall muss die zivile Verteidigung weiter gestärkt
106 werden. Wir setzen uns für ein Sonderprogramm für die zivile Verteidigung ein, um nationale
107 Reserven zu verstärken, den Schutz vor chemischen, biologischen, radiologischen und
108 nuklearen Substanzen zu erhöhen, Lücken in der Warninfrastruktur zu schließen und sowohl
109 das Technische Hilfswerk als auch das BBK der veränderten Lage entsprechend zu finanzieren.

110 Es braucht ein Schutzraumkonzept und ein Konzept zum Aufbau einer „Zivilschutzreserve“,
111 sogenannte Spontanhelfer müssen besser eingebunden werden. An regelmäßig stattfindenden
112 Großübungen zur Krisenbewältigung halten wir fest.

113 Dank der CDU-geführten Bundesregierung wird erstmals der physische Schutz kritischer
114 Infrastrukturen bundeseinheitlich und sektorenübergreifend in den Blick genommen. Mit dem
115 KRITIS-Dachgesetz wird Deutschland gegen Krisen und Angriffe widerstandsfähiger. Es
116 werden einheitliche Mindeststandards, Risikoanalysen und ein Störungsmonitoring
117 geschaffen. Damit sollen die Abwehrfähigkeit und die Resilienz unserer kritischen
118 Infrastrukturen, wie Energie, Ernährung, Wasser, Gesundheit, Transport und Verkehr,
119 gehärtet werden. Für einen verbesserten, umfassenden Schutz der kritischen Infrastrukturen
120 wird auch die sogenannte NIS-2-Richtlinie in deutsches Recht umgesetzt.

121 Bevölkerungsschutz ist eine gesamtgesellschaftliche Aufgabe, die ohne das Engagement
122 Freiwilliger nicht zu bewältigen ist. Es bedarf einer bundesweiten Kampagne zur Förderung
123 ehrenamtlicher Tätigkeiten, die sowohl die Bedeutung des Ehrenamts in der Gesellschaft
124 hervorhebt als auch konkrete Anreize setzt.

125 Die Fähigkeiten der Bevölkerung zu Selbstschutz und Selbsthilfe gilt es zu stärken. Damit
126 erhöht sich die Resilienz der Gesellschaft insgesamt. Bürgerinnen und Bürger sollen im
127 Krisenfall in der Lage sein, sich selbst und einander zu helfen. Dies erfordert eine breit
128 angelegte Informations- und Aufklärungskampagne, die über Notfallvorsorge,
129 Selbsthilfemaßnahmen und Erste-Hilfe-Kenntnisse aufklärt.

130 Die Bundeswehr verfügt im Katastrophen- und Bevölkerungsschutz über wichtige und
131 unverzichtbare Fähigkeiten. Soldatinnen und Soldaten sollen auch in Zukunft außerhalb ihres
132 Kernauftrages im Rahmen der Amtshilfe bereitstehen können und die Arbeit der
133 Rettungsdienste und Feuerwehren, des Katastrophenschutzes und der Polizei wirksam
134 ergänzen.

135 **Drohnen aufspüren und abwehren**

136 Drohnen verändern grundlegend die Art, wie Kriege geführt werden. Das sehen wir leider
137 täglich im Angriffskrieg Russlands gegen die Ukraine. Nun spielen sie auch eine bedrohliche
138 Rolle am bislang friedlichen europäischen Himmel jenseits der Ukraine. Sie dringen in den
139 europäischen Luftraum ein, legen den Flugverkehr in Skandinavien und bei uns in
140 Deutschland lahm. Tausende Reisende bleiben stecken, wirtschaftliche Schäden in
141 Millionenhöhe entstehen. Kritische Infrastrukturen werden ausspioniert. Es zeigt sich auch
142 hier, dass sich innere und äußere Sicherheit nicht trennen lassen. Zur bitteren Wahrheit
143 gehört: Deutschland hat sich lange schwer damit getan, die Realität zu erkennen, und die
144 Bedeutung von Drohnen unterschätzt. Es braucht daher jetzt einen integrierten Ansatz für die
145 Abwehr und den Einsatz von Drohnen. Und das heißt neben technischen und finanziellen
146 Voraussetzungen zuallererst: klare Zuständigkeiten und Regelungen.

147 In einem ersten, wichtigen Schritt ist dies im Kabinettsbeschluss zum neuen
148 Bundespolizeigesetz festgelegt. Die Bundespolizei darf danach künftig eigene Drohnen zur
149 Überwachung und Aufklärung einsetzen, etwa bei Großveranstaltungen oder zur Kontrolle
150 schwer zugänglicher Bahnstrecken. Zugleich erhält sie Befugnisse zur Abwehr von Drohnen.
151 Dazu zählen technische Maßnahmen wie elektromagnetische Impulse, GPS-Störungen oder
152 physische Eingriffe. Ebenso ist es richtig, bei der Bundespolizei eine eigene
153 Drohnenabweereinheit aufzustellen.

154 Ergänzend muss das Luftsicherheitsgesetz angepasst werden, damit die Bundeswehr bei
155 bestimmten Drohnengefahren Amtshilfe leisten kann – etwa bei der Ortung militärischer
156 Drohnen in großer Höhe oder beim Abschuss von Drohnen als ultima ratio.

157 Wir müssen Drohnen ernst nehmen. Diese Gefahr von oben ist eine junge Technik, und sie wird
158 sich wie andere Kampftechniken dynamisch weiterentwickeln. Das zeigt auch und gerade
159 Russlands Angriffskrieg gegen die Ukraine. Für uns ist klar: Soldaten der Bundeswehr sollen
160 durch Aus- und Weiterbildungsprogramme von den Erfahrungen der ukrainischen Streitkräfte
161 im Drohnenkampf profitieren können.

162 Wir müssen den Rüstungsstandort Deutschland stärken. Unser Land muss führend werden bei
163 der Entwicklung und Produktion von Drohnen. Jederzeit muss der Zugriff auf das aktuell
164 wichtigste Waffensystem gewährleistet sein.

165 **Vor Fake-News und Desinformation schützen, demokratische Resilienz stärken**

166 Neben Spionage, Sabotage und Cyberangriffen sind gezielte Desinformationen ein
167 wesentlicher Teil hybrider Bedrohungen. Die gezielte Verbreitung von Fake-News ist ein
168 schleichendes Gift für den Zusammenhalt unserer Gesellschaft, erschüttert das Vertrauen in
169 die Funktionsfähigkeit unseres Staates und gefährdet den offenen Dialog, der für unsere
170 Demokratie unerlässlich ist.

171 Polarisierung und Destabilisierung sind reale Gefahren für unsere Demokratie. Es liegt an uns,
172 ihre Abwehrkräfte zu stärken. Das heißt zuallererst: Unsere Behörden müssen ihre
173 Maßnahmen gegen die zunehmende gezielte Einflussnahme und Desinformation durch
174 ausländische und inländische Akteure verstärken und einen noch engeren Austausch
175 sicherstellen. Zugleich ist es wichtig, dass wir noch wachsamer werden. Wir brauchen
176 Gegenmaßnahmen, um Desinformation für jedermann erkennbar zu machen.

177 Gleichzeitig sind wir uns bewusst, dass unser Staat im Zuge von Desinformationskampagnen
178 anderer Länder diffamiert wird. Die Manipulation der öffentlichen Meinung erfolgt nicht nur in
179 den Sozialen Medien, sondern auch über offizielle Kanäle autokratischer Regime. Diese
180 Rufschädigung kann die deutsche Außenpolitik, Entwicklungszusammenarbeit und etablierte
181 Beziehungen langfristig schwer beeinträchtigen.

182 Umso mehr müssen wir Deutschland von innen heraus stärken. Wer sich bewusst zum Helfer
183 autoritärer Regime macht, gefährdet unsere Demokratie, unser aller Sicherheit und Freiheit.
184 Deshalb muss im Netz entschieden gegen diejenigen vorgegangen werden, die sich freiwillig
185 und wissentlich zu Handlangern von Staaten und Organisationen machen, die unsere
186 freiheitlich-demokratische Ordnung untergraben. Wir stellen uns gegen politische oder
187 religiös motivierte Akteure, die die Sorgen und Ängste der Menschen für die Verbreitung ihrer
188 Ideologien missbrauchen. Unser Augenmerk ist dabei gerade auch auf die gezielte
189 Einflussnahme auf Wahlen, auf Parlamente oder auf vulnerable Gruppen gerichtet.

190 Auch extremistische Gefährdungen lauern immer mehr im Netz, nicht nur auf der Straße.
191 Extremisten muss es schwerer gemacht werden, ihr Gedankengut zu verbreiten. Denn häufig
192 dienen Soziale Netzwerke als Keimzelle extremer politischer oder religiöser Gruppierungen.
193 Um Netzwerke zu erkennen und zu zerschlagen, müssen wir auch hier die Zusammenarbeit
194 zwischen Justiz- und Sicherheitsbehörden in ganz Europa stärken und deren Kompetenzen
195 ausbauen. Verwaltungsstellen müssen auf europäischer Ebene besser vernetzt und

196 Nachrichtendienste in ihren technischen Möglichkeiten langfristig besser ausgestattet
197 werden.

198 Es ist richtig, Bots und Fake-Accounts zu verbieten, denn sie verzerren die öffentliche
199 Wahrnehmung und spielen den politischen Rändern in die Hände. Gleichzeitig müssen mehr
200 Möglichkeiten geschaffen werden, Gleiches mit Gleichem zu bekämpfen: Algorithmen, die
201 Falschinformationen oder Deepfakes verbreiten, können nur von Algorithmen und Künstlicher
202 Intelligenz in Echtzeit erkannt, gemeldet und richtiggestellt werden.

203 Alle demokratischen Staaten Europas sehen sich gleichermaßen mit den Bedrohungen durch
204 Desinformation konfrontiert. Entsprechend müssen Maßnahmen zu ihrer Bekämpfung
205 innerhalb der Europäischen Union weiterhin gemeinschaftlich angegangen werden. Betreiber
206 von Social-Media-Plattformen wie Meta oder TikTok werden durch den Digital Services Act
207 (DSA) in die Verantwortung genommen. Sie dürfen sich der europäischen Gesetzgebung nicht
208 entziehen. Wenn Social-Media-Plattformen in Europa Geschäfte machen wollen, müssen sie
209 auch unsere Gesetze einhalten. Hier darf es keine Kompromisse geben. Die EU-Kommission
210 muss die DSA-Verfahren gegen die sehr großen Online-Plattformen zügig abschließen. Sie
211 müssen ihre Black Boxes öffnen, Transparenz herstellen und aufhören, das Melden von Fake
212 News zu erschweren. Der Digital Services Coordinator (DSC) bei der Bundesnetzagentur, der
213 überwacht, dass Online-Dienste die Regeln des DSA einhalten, muss personell besser
214 ausgestattet werden. Gleichzeitig muss das Beschwerdeportal für Nutzer beim DSC bekannter
215 gemacht werden.

216 Weil Bürgerinnen und Bürger mehr denn je auf zuverlässige und unabhängige
217 Informationsquellen zurückgreifen können müssen, sind europäische Medienformate weiter
218 auszubauen. Ebenfalls muss Aufklärungsarbeit geleistet werden, damit Nutzer Deepfakes
219 erkennen können.

220 Anfeindungen und Drohungen im Netz führen bei Betroffenen zum Rückzug aus politischen
221 Debatten. Wir machen uns dafür stark, dass Respekt und Sachlichkeit auch im Netz nicht
222 verloren gehen. Hier werden sowohl Beratungsangebote, faire, digital moderierte
223 Streitkulturen als auch eine effiziente Strafverfolgung benötigt. Was sich im Internet abspielt,
224 ist Realität und muss sich analog im Strafrecht widerspiegeln. Das Erstellen und Teilen von
225 Beiträgen, die Drohungen verbreiten, fällt nicht unter den Schutz der Meinungsfreiheit.
226 Anonymität im Netz darf nicht vor Konsequenzen schützen.

227 Sicherheit ist die Voraussetzung dafür, dass wir in Freiheit leben können. Wir müssen unsere
228 Sicherheit und unsere Freiheit vor Anfeindungen und Angriffen jeder Art schützen. Immer
229 häufiger bedeutet das: Wir müssen uns auch vor Feinden schützen, die im Verborgenen

230 angreifen, sich tarnen und ihre Spuren verwischen. Die Gefahren, die von ihnen für unser Land
231 ausgehen, dürfen wir nicht unterschätzen. Wir werden auf die Probe gestellt und auf
232 Schwächen getestet. Deshalb brauchen wir neue Fähigkeiten der Aufklärung und der Abwehr.
233 Unsere Antwort ist klar: Wir werden Deutschland sicherer und widerstandsfähiger machen.

ENTWURF
Tabletop
Media