Berliner Erklärung

Deutschland sicherer und widerstandsfähiger machen – hybride Bedrohungen und Angriffe koordiniert und wirksam abwehren

Beschluss des Bundesvorstandes der CDU Deutschlands
Berlin, 20. Oktober 2025

Viele Menschen und Betriebe 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, gezielte Desinformationskampagnen, 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 und Betriebe 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. Wir begrüßen, dass sich der NSR in seiner ersten Sitzung schwerpunktmäßig mit hybriden Bedrohungen beschäftigen wird und hierzu einen ressortübergreifenden Aktionsplan auf den Weg bringt.

Wir wissen: Hybride Angreifer wollen immer auch testen, wie sehr wir bereit sind, uns zu verteidigen und unser Land zu schützen. Wir sind bereit, alles zu tun, was nötig ist. Sicherheit ist nicht nur Abwehr, sie ist auch Ausdruck von Stärke, von Vertrauen in die eigenen

Fähigkeiten. Deutschland muss wehrhaft bleiben, widerstandsfähiger werden und schneller reagieren können.

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

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

Gefahren aus dem Cyberraum abwehren

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

Um auf diese dynamischen Entwicklungen angemessen reagieren zu können, müssen wir unsere Verteidigungsfähigkeit und Resilienz fortwährend weiter erhöhen. Dabei ist entscheidend, dass unsere Sicherheitsbehörden bei der Cyberabwehr mit den notwendigen Befugnissen, Fachpersonal und moderner Infrastruktur ausgestattet werden und gut vernetzt zusammenarbeiten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) muss in enger Abstimmung mit den Ländern zu einer Zentralstelle für Fragen der Informations- und Cybersicherheit ausgebaut werden und als Ausbaumaßstab vorbildliche Strukturen in den Bundesländern (insbesondere Hessen) zugrunde legen. So bekommt Deutschlands Cybersicherheitsarchitektur neben dem Bundesamt für Verfassungsschutz und dem Bundeskriminalamt eine starke dritte Säule. Das Nationale Cyber-Abwehrzentrum muss so weiterentwickelt werden, dass es im Zusammenspiel mit dem NSR in komplexen Schadenslagen, wie etwa bei einem Angriff auf ein Satellitennetzwerk, bundesweit eine Abwehr von Gefahren und Angriffen koordinieren kann.

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

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

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

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

Bevölkerungsschutz stärken, kritische Infrastrukturen widerstandsfähiger machen

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

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

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

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

Es braucht ein Schutzraumkonzept, das ähnlich wie z.B. in Finnland verschiedene Lebensbereiche gemeinsam denkt und nutzbar macht (Schutzräume, die in Friedenszeiten für soziale Zwecke, Sport und Freizeit genutzt werden können), und ein Konzept zum Aufbau einer „Zivilschutzreserve“; sogenannte Spontanhelfer müssen besser eingebunden werden. An regelmäßig stattfindenden Großübungen zur Krisenbewältigung halten wir fest.

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

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

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

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

Drohnen aufspüren und abwehren

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

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

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

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

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

Vor Fake-News und Desinformation schützen, demokratische Resilienz stärken

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

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

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

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

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

Nachrichtendienste in ihren technischen Möglichkeiten langfristig besser ausgestattet werden.

Bots sind schnellstmöglich aus dem Netz zu entfernen, denn sie verzerren die öffentliche Wahrnehmung und spielen den politischen Rändern in die Hände. Gleichzeitig müssen mehr Möglichkeiten geschaffen werden, Gleiches mit Gleichem zu bekämpfen: Algorithmen, die Falschinformationen oder Deepfakes verbreiten, können nur von Algorithmen und Künstlicher Intelligenz in Echtzeit erkannt, gemeldet und richtiggestellt werden.

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

Weil Bürgerinnen und Bürger mehr denn je auf zuverlässige und unabhängige Informationsquellen zurückgreifen können müssen, sind europäische Medienformate weiter auszubauen. Eine vielfältige Medienlandschaft und professioneller Journalismus – ob öffentlich-rechtlich oder privat finanziert – sind unerlässliche Grundlage des öffentlichen Diskurses. Ebenfalls muss Aufklärungsarbeit geleistet werden, damit Nutzer Deepfakes erkennen können.

Anfeindungen und Drohungen im Netz führen bei Betroffenen zum Rückzug aus politischen Debatten. Wir machen uns dafür stark, dass Respekt und Sachlichkeit auch im Netz nicht verloren gehen. Hier werden sowohl Beratungsangebote, faire, digital moderierte Streitkulturen als auch eine effiziente Strafverfolgung benötigt. Was sich im Internet abspielt, ist Realität und muss sich analog im Strafrecht widerspiegeln. Das Erstellen und Teilen von Beiträgen, die Drohungen verbreiten, fällt nicht unter den Schutz der Meinungsfreiheit. Anonymität im Netz darf nicht vor Konsequenzen schützen. Gerade für Kinder und Jugendliche gilt im Netz ein besonderer Schutzauftrag. Wir prüfen, wie sich eine wirksame Altersverifikation umsetzen lässt.

Sicherheit ist die Voraussetzung dafür, dass wir in Freiheit leben und wirtschaften können. Wir müssen unsere Sicherheit und unsere Freiheit vor Anfeindungen und Angriffen jeder Art schützen. Immer häufiger bedeutet das: Wir müssen uns auch vor Feinden schützen, die im Verborgenen angreifen, sich tarnen und ihre Spuren verwischen. Die Gefahren, die von ihnen für unser Land ausgehen, dürfen wir nicht unterschätzen. Wir werden auf die Probe gestellt und auf Schwächen getestet. Deshalb brauchen wir neue Fähigkeiten der Aufklärung und der Abwehr. Unsere Antwort ist klar: Wir werden Deutschland sicherer und widerstandsfähiger machen.