Deutscher Bundestag **Drucksache 21/6653**

21. Wahlperiode 23.06.2026

Antrag

der Abgeordneten Donata Vogtschmidt, Clara Bünger, Anne-Mieke Bremer, Katrin Fey, Dr. Gregor Gysi, Luke Hoß, Ferat Koçak, Jan Köstering, Sonja Lemke, Bodo Ramelow, David Schliesing, Aaron Valent, Christin Willnat und der Fraktion Die Linke

Gegen die Einführung von Hackbacks und offensiver Cyberabwehr

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Eine Zeitenwende in der inneren Sicherheit und der Ausbau aktiver Cyberabwehr wurde bereits mit Koalitionsvertrag vom Mai 2025 angekündigt. Mit dem vorliegenden Gesetzentwurf der Bundesregierung zur Stärkung der Cybersicherheit soll dieses Vorhaben umgesetzt werden. Die Grenzen des „verfassungsrechtlich Möglichen“ (Koalitionsvertrag, Z. 2679) werden dabei entgegen der Vereinbarung jedoch klar überschritten.

Mit dem vorliegenden Entwurf soll für Bundeskriminalamt (BKA) und Bundespolizei die Fähigkeit geschaffen werden, zur Abwehr von Cybergefahren Daten in IT-Systemen auszulesen, zu verändern und zu löschen, sowie Datenverkehr umzulenken und mitzulesen. Dies bedeutet einen massiven Eingriff in informationstechnische Systeme, dem weder ein Richtervorbehalt noch ausreichende parlamentarische Kontrolle als grundrechtssichernde Mechanismen zur Seite gestellt werden. Nach Ansicht von Bundesinnenminister Dobrindt stehe der Gesetzentwurf unter dem Motto „Wir schlagen zurück“; mit ihm soll die IT-Infrastruktur von Angreifern gestört und zerstört werden (https://taz.de/Gesetzentwurf-zur-Cybersicherheit/!6182259/). Der Gesetzentwurf ist getragen vom Gedanken der technischen Machbarkeit. Grund- und völkerrechtliche Schranken sowie negative Chilling Effects der zahlreichen Eingriffsbefugnisse stehen dahinter deutlich zurück.

Die Bundesregierung vermeidet in dem Zusammenhang den Begriff „Hackback“, weil dieser auch Maßnahmen umfassen „könnte, die nach deutscher Rechtsordnung oder völkerrechtlich nicht zulässig sind“ (vgl. Antwort auf Frage 22 auf Ds 21/1482). Während der Bundesinnenminister Hackbacks als Vergeltungsschlag von Maßnahmen der Gefahrenabwehr unterscheiden möchte, kamen die Wissenschaftlichen Dienste (WD) des Bundestags zu einem anderen Ergebnis: Offensive Abwehr lasse sich von Angriffswerkzeugen nicht unterscheiden, stellten sie in einer eingestuften Ausarbeitung von 2019 fest, die auf Netzpolitik.org veröffentlicht wurde (https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/). Zulässig könnten derartige Maß-

nahmen für die Bundeswehr sein, jedoch nur zur Selbstverteidigung im militärischen Sinne. Niedrigschwellig agierende Angreifer ließen sich damit jedoch nicht stoppen, offensive Cyberabwehr führe außerdem zu einem verschärften Rüstungswettlauf. In einem aktuellen Gutachten stellen die WD fest, dass Maßnahmen der aktiven Cyberabwehr stets am Völkerrecht zu messen sind, sobald sie die völkerrechtlich geschützte Sphäre anderer Staaten tangieren und den Gewaltbegriff i. S. v. Art. 2 Ziff. 4 VN-Charta erfüllen, und dass das Recht zur Selbstverteidigung dann nur in Ausnahmefällen eröffnet ist (https://www.die-linke-thueringen.de/fileadmin/DonataVogtschmidt/Dokumente/2026/260622_WD_aktive_Cyberabwehr_Hackbacks_Voelkerrecht.pdf).

Der vorliegende Gesetzentwurf ignoriert konsequent die Möglichkeit, dass Maßnahmen einer „aktiven Cyberabwehr“ auf Eingriffe in fremde staatliche IT-Infrastruktur hinauslaufen können, und setzt sich mit den Folgen nicht auseinander: So heißt es in der Entwurfsbegründung, um „Gefahrenlagen wirksam abzuwehren“, sei es erforderlich, „Schwachstellen in der Informationstechnik der Angreiferinfrastrukturen zu suchen, die Infrastruktur (…) möglichst umfassend aufzuklären (…)“ und „sofern technisch umsetzbar, auch unmittelbaren Zugriff auf die Inhalte des Servers bzw. das Angreifernetzwerk zu erhalten“. (S. 49 auf BR-Drs. 323/46). Erst im Ergebnis ist dann aber feststellbar, ob militärische oder staatliche IT-Systeme oder solche einer Kritischen Infrastruktur in das Angreifernetzwerk eingebunden sind und ob damit völker- oder verfassungsrechtliche Schwellen verbunden sind. Dies erfolgt unabhängig von der Schwierigkeit, ob der Angriff auch den Betreibern dieser IT-Systeme zurechenbar sind oder sie selbst Opfer der Angreifer sind, die ihre Systeme als Proxy-Server missbrauchen.

Der Gesetzentwurf zur Stärkung der Cybersicherheit möchte dennoch entsprechende Befugnisse für Polizeibehörden schaffen.

Mit diesem Antrag werden offensive Angriffe gegen fremde IT-Systeme grundsätzlich abgelehnt. Solche Angriffe setzen eine vorherige Aufklärung des Zielsystems und teilweise das Geheimhalten von IT-Schwachstellen voraus und gefährden so die allgemeine IT-Sicherheit erheblich. Dies kann auch Kritische Infrastrukturen in Deutschland betreffen, insbesondere wenn sie zur Durchführung von digitalen Angriffen genutzt werden oder mit den neu zu schaffenden Befugnissen von BKA und Bundespolizei sogar abgeschaltet werden, ohne dass die Betroffenen darüber informiert werden. Auch gegen das mit dem Gesetzentwurf vorgesehene massenhafte „Patchen“ von infizierten IoT-Geräten oder Routern bestehen grundrechtliche und technische Bedenken. Cybersicherheit ist nur global und gemeinsam erreichbar und kann auch nicht gegen andere, sondern nur mit anderen Staaten durchgesetzt werden.

Laut Koalitionsvertrag soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Zentralstelle für Fragen der Informations- und Cybersicherheit ausgebaut werden. Dem vorliegenden Gesetzentwurf zur Stärkung der Cybersicherheit nach sollen von den dafür geplanten beträchtlichen Haushaltsausgaben von fast 60 Millionen € pro Jahr jedoch nur 5 Prozent dem BSI zufallen. Der deutlich größere Anteil soll für Aufgaben der Polizeibehörden aufgewendet werden. Damit werden selbst im Sinne des Koalitionsvertrags die Prioritäten falsch gesetzt.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. laufende Gesetzesvorhaben nicht weiter zu betreiben, die Hackbacks oder vergleichbare Maßnahmen der offensiven Cyberabwehr gesetzlich verankern würden;
2. laufende Gesetzesvorhaben nicht weiter zu betreiben, die dem BKA und der Bundespolizei ermöglichen, zur Abwehr von Cybergefahren ohne Wissen

der Betroffenen in IT-Systeme einzudringen und diese auszulesen, zu verändern oder zu löschen;

3. laufende Gesetzesvorhaben nicht weiter zu betreiben, die DNS-Anbieter und Digitale Dienste zur Umleitung von Datenverkehr an das BKA und die Bundespolizei verpflichten könnten, insbesondere wenn sie hierdurch diesen massenhaft Zugang zu Datenverkehr und Kommunikationsinhalten verschaffen würden;
4. einen Gesetzentwurf vorzulegen, der die defensive IT-Sicherheit mit den notwendigen Ressourcen insbesondere für das BSI stärkt, indem unter anderem
   a) das BSI ermächtigt wird, die Hosting-Provider auch präventiv zum Einspielen verfügbarer Sicherheitsupdates zu verpflichten, wenn es sich um Einrichtungen des Bundes oder um Betreiber*innen wichtiger oder besonders wichtiger Einrichtungen handelt,
   b) das BSI die Befugnis erhält, gegenüber DNS-Anbietern die Umleitung von Datenverkehr anzuordnen, sofern dies für die Öffentlichkeit nachvollziehbar dokumentiert wird und eventuell beim BSI abgefangene Daten strengen Zweckbindungs- und Löschfristen unterliegen;
5. das BSI zu verpflichten, dem Deutschen Bundestag einmal im Jahr über seine Aktivitäten im Rahmen dieser neuen Aufgaben zu berichten.

Berlin, den 23. Juni 2026

Heidi Reichinnek, Sören Pellmann und Fraktion

Begründung

Maßnahmen der offensiven Cyberabwehr können eine massive Gefährdung der allgemeinen IT-Sicherheit mit sich bringen, unabhängig davon, ob sie als ‚Hackbacks' bezeichnet werden. Vor dem Beginn des eigentlichen Einsatzes ist eine umfassende Aufklärung des Täterumfelds erforderlich. Das konterkariert das Konzept der gewünschten schnellen Reaktion durch eine offensive Maßnahme. Das für eine wirksame offensive Cyberabwehr erforderliche Aufklären des Täterumfelds könnte Begehrlichkeiten des präventiven Kompromittierens fremder IT-Systeme in unverhältnismäßiger Weise zu diesem Zweck anregen. Laut Begründung des vorliegenden Gesetzentwurfs sollen auch abgefangene oder der Polizei vorliegende Zugangsdaten oder IT-Schwachstellen genutzt werden dürfen. Daraus ergibt sich zwangsläufig ein Interesse der Polizei an nicht-geschlossenen IT-Schwachstellen und eine entsprechende Gefährdung der allgemeinen IT-Sicherheit. Dies läuft der IT-Sicherheitsforderung, dass Schwachstellen so schnell wie möglich geschlossen werden sollen zuwider und ist daher abzulehnen. Neue Schwachstellen (Zero-Days) müssen so schnell wie möglich dem Hersteller gemeldet und geschlossen werden. Bei bekannten Schwachstellen muss so schnell wie möglich ein entsprechendes update bei den Betroffenen eingespielt werden.

Weiterhin bleibt im Gesetzentwurf unbeachtet, dass das Problem der Attribution nicht gelöst ist. Darin liegt ein Kernproblem aktiver Cyberabwehr, wie die AG KRITIS in ihrer Stellungnahme zum Referentenentwurf ausführte (https://ag.kritis.info/wp-content/uploads/2026/03/20260311-AG_KRITIS_Stellungnahme_Cyberabwehr_-_final.pdf). Eine zuverlässige Identifizierung von Angreifern braucht Zeit. Das Risiko für unbeabsichtigte Attacken und Kollateralschäden ist entsprechend hoch, ebenso für den Missbrauch des Angriffs fremder IT-Systeme mit politisch getriebenen Mutmaßungen oder Interessen. Zudem verhindert das Attributionsproblem eine Abgrenzungsmöglichkeit zum Zuständigkeitsbereich der Länder und insbesondere der Bundeswehr, weshalb es höchst

zweifelhaft erscheint, dass für Hackbacks durch die Polizei eine haltbare Rechtsgrundlage geschaffen werden kann. Auch Nachrichtendienste sollten operative Fähigkeiten vor dem Eindruck der deutschen Geschichte nicht erlangen dürfen (https://www.bundestag.de/resource/blob/1136072/WD-3-089-25.pdf), und sollte die Bundeswehr Hackbacks anwenden, würden diese Einsätze einem Zustimmungsvorbehalt des Parlaments unterliegen. Das Problem der Attribution und der Gefährdung der allgemeinen IT-Sicherheit wäre jedoch auch in dem Fall ungelöst. Die Bedrohungs- und Angriffsspirale kann sich deshalb leicht aufschaukeln, bis hin zu einem konventionellen militärischen Konflikt. Deshalb werden Hackbacks in diesem Antrag vollständig abgelehnt, unabhängig von der Frage, welche Behörde dazu ermächtigt werden soll, sie anzuwenden (Forderung 1).

Jene Teile des Gesetzentwurfs zur Stärkung der Cybersicherheit, die sich auf Änderungen des BSI-Gesetzes beziehen, sind zum Teil durchaus zu begrüßen. Sie enthalten Maßnahmen zur Verbesserung der defensiven Cyberabwehr, unter anderem zur verbesserten Schadprogrammerkennung und erweiterte Informationspflichten von Dienstanbietern gegenüber dem BSI, was einem besseren Cyber-Lagebild zuträglich wäre. Auch soll das BSI bereits vor dem Eintreten eines Schadenfalls aktiv werden dürfen und gefährdete Anbieter*innen unterstützen. Forderung 4 dieses Antrags zielt darüber hinaus auf das Problem ab, dass bekannte, kritische IT-Schwachstellen von vielen Kunden der Hosting-Provider oft erst sehr verzögert geschlossen werden, was insbesondere bei Betreiber*innen wichtiger und besonders wichtiger Einrichtungen (Auflistung in den Anlagen 1 und 2 des BSI-Gesetzes) und in der Bundesverwaltung ein hohes Risiko für die Cybersicherheit und Resilienz der Gesellschaft birgt. Deshalb soll das BSI in derartigen Fällen die Möglichkeit bekommen, Hosting-Provider zum Einspielen verfügbarer Sicherheitsupdates verpflichten zu können. Das geheime Eindringen in IT-Systeme und deren Manipulation durch Polizeien ist hingegen aufgrund mangelnder Transparenz, der großen Eingriffstiefe und des großen Missbrauchspotenzials grundsätzlich abzulehnen (Forderung 2), zumal dies laut Gesetzesentwurf ohne Wissen der Betroffenen – das schließt die Kunden eines Providers ein – erfolgen darf. Die Erforderlichkeit ist jedenfalls nicht ersichtlich und das BSI könnte der Aufgabe in Zusammenwirken mit den Hosting-Providern angemessener nachkommen (Forderung 4). Ebenso verhält es sich mit der defensiven Cyber-Maßnahme, Datenverkehr auf DNS-Ebene umzuleiten (Forderung 3). Das ist im Gesetzentwurf in der Hand der Polizei problematisch, weil eine Umlenkung des Datenverkehrs auf polizeilich kontrollierte Systeme explizit vorgesehen ist. Der IT-Wirtschaftsverband eco wertet dies als ein scharf abzulehnendes Eingriffspotenzial, das strukturell für die zentrale Beeinflussung von Kommunikationsflüssen und zur Inhaltslenkung missbraucht werden könnte. Vergleichbare Initiativen gebe es unter anderem in Russland und in der Türkei. (https://www.golem.de/news/gesetzentwurf-zu-hackbacks-eco-warnt-vor-gesetzen-wie-in-russland-und-der-tuerkei-2603-206011.html).