

Regierungsentwurf zur Stärkung der Cybersicherheit beraten Lob und Kritik zum Cyberabwehr-Gesetzentwurf

5.10.2026 - | Deutscher Bundestag

Das Parlament hat am Donnerstag, 25. Juni 2026, den von der Bundesregierung eingebrachten Gesetzentwurf „zur Stärkung der Cybersicherheit“ (21/6585(Dokument, öffnet ein neues Fenster), 21/7406(Dokument, öffnet ein neues Fenster)) in erster Lesung beraten. Im Anschluss an die Debatte wurde der Entwurf gemeinsam mit einem Antrag der Fraktion Die Linke „gegen die Einführung von Hackbacks“ (21/6653(Dokument, öffnet ein neues Fenster)) in die Ausschüsse überwiesen. Federführend bei den weiteren Beratungen wird der Innenausschuss sein. Zeit: Montag, 5. Oktober 2026, 14 Uhr Ort: Berlin, Paul-Löbe-Haus, Sitzungssaal E 800 Die Sitzung ist öffentlich und wird auf www.bundestag.de übertragen.

Von einem „Meilenstein der Sicherheitsarchitektur in Deutschland“ sprach **Bundesinnenminister Alexander Dobrindt (CSU)** zu Beginn der Debatte. „Mit diesem Gesetzesentwurf legen wir den Schalter um: Von der Aufklärung, hin zur Abwehr“, sagte Dobrindt.

Indem die Grundlagen für eine aktive Cyberabwehr gelegt würden, mache man unmissverständlich klar: Deutschland handle entschlossen, wenn es um die Verteidigung im Cyberraum geht. „Wer uns zukünftig im Cyberraum angreift, der muss wissen: Wir schlagen zurück und sind in der Lage, die Angreifer in ihrer Infrastruktur zu stören und zu zerstören“, sagte der Innenminister.

Steffen Janich (AfD) teilt die Problemanalyse im Gesetzentwurf, die „erfrischend ehrlich und schonungslos“ sei. Deutschland stehe in der Tat im Fokus hochprofessioneller Cyberangriffe. Auch sei es richtig, dass Deutschlands wirtschaftlicher Erfolg und seine nationale Sicherheit mit Cybersicherheit untrennbar verbunden sind.

Gleichwohl gebe es noch Handlungsbedarf, so Janich. Wenn etwa die Bundespolizei dem Betreiber eines IT-Systems dessen Nutzung untersagt, müsse dies befristet sein. Unternehmen sei nicht geholfen, wenn die Insolvenz wegen eines Cyberangriffes verhindert wird, sie dann aber aufgrund einer Nutzungsuntersagung eintritt. Hier müsse nachjustiert werden, forderte der AfD-Abgeordnete, der dem Innenminister vorwarf, beim Thema Hackbacks vollständig eingeknickt zu sein. Man müsse bei Cyberangriffen von „Schurkenstaaten“ mit Vergeltungsschlägen gegen deren IT-Struktur reagieren dürfen, sagte Janich.

Deutschland müsse bei der Abwehr von Angriffen im Cyberraum gut aufgestellt sein, betonte **Daniel Baldy (SPD)**. Die Sicherheitsbehörden dürften nicht nur am Rand stehen, Cyberangriffe beobachten „und danach erklären, was alles hätte besser laufen können“. Sie müssten nicht nur aufklären, sondern auch abwehren können. Baldy verwies auf die Heterogenität der Angreifer, die mal privat, mal halb-staatlich und mal staatlich seien. „Deshalb stärken wir mit diesem Gesetz nicht nur eine Sicherheitsbehörde, sondern wir geben BSI, BKA und Bundespolizei die richtigen Werkzeuge an die Hand, damit sie zukünftig angemessen auf Cyberangriffe reagieren können“, sagte der SPD-Abgeordnete.

Ziel müsse es nicht nur sein, laufende Angriffe zu stoppen, sondern den entstandenen Schaden so gering wie möglich zu halten. Deshalb sei es richtig, dass BKA und Bundespolizei in Zukunft auch

die Möglichkeit haben, durch Cyberangriffe abgeflossene Daten zu löschen oder zu verändern. Es gehe nicht um Harakiri und nicht um Hackbacks. „Es geht darum, nicht tatenlos zuzusehen, wie die Verbrecher mit der Beute davonlaufen“, sagte Baldy.

Das Innenministerium lasse mit dem Gesetzentwurf ganz zentrale Fragen unbeantwortet, befand **Marcel Emmerich (Bündnis 90/Die Grünen)**. Deutschland brauche dringend mehr Cybersicherheit, machte er deutlich. „Wir müssen unsere Freiheit und Demokratie schützen, wir müssen wehrhaft sein.“ Bei Gesetzen an der Schnittstelle von Innen- und Digitalpolitik zeigt sich laut Emmerich aber immer wieder dasselbe Problem. „Das Innenministerium fremdelt einfach allein schon mit der digitalen Bedrohungslage.“

Künftig solle der Staat nicht nur verteidigen, sondern selbst aktiv in fremde IT-Systeme eindringen, Daten verändern und löschen oder den Datenverkehr umleiten können. „Das ist eine neue Qualität und die steht mit diesem Entwurf nicht auf rechtssicheren Füßen“ sagte der Grünenabgeordnete. Der Entwurf gebe zudem mehreren Behörden weitreichende Eingriffsbefugnisse, beantworte aber nicht die Frage, wer im Ernstfall das Sagen hat und wer die Verantwortung trägt, wenn aufgrund einer fehlerhaften Zuschreibung nicht der Angreifer, sondern der Server einer eigenen KRITIS-Anlage getroffen wird.

Aus Sicht von **Donata Vogtschmidt (Die Linke)** versucht Bundesinnenminister Dobrindt den Begriff der aktiven Cyberabwehr so zu framen, „dass man den Begriff Hackback, um den es hier heute eigentlich geht, vergisst“. Der Minister stehe aber mit seiner Auffassung allein. Von der Zivilgesellschaft über die Wissenschaft bis hin zu Wirtschaftsverbänden sei man sich einig: Was hier als aktive Cyberabwehr verkauft werde, seien schlicht und ergreifend Hackbacks, die keine Verteidigungshandlung darstellten.

Bei einem Hackback, so Vogtschmidt, gehe es um einen aktiven Gegenangriff auf eine Cyberattacke, bei dem in das System des Angreiferetzes eingedrungen werde, um es zu zerstören oder auszuschalten. Das Problem dabei sei, das für einen erfolgreichen Gegenangriff das Umfeld des Angreifers aufgeklärt werden müsse - etwa durch erbeutete Zugangsdaten oder IT-Schwachstellen. Dies benötige eine Menge Vorlauf und bedeute schlicht das „Hacken auf Verdacht“ bei fremden IT-Systemen, um im Falle eines Angriffs einen erfolgversprechenden Hackback durchführen zu können. „Das klingt nicht nur illegal und unsicher. Das ist es auch“, urteilte die Linken-Abgeordnete.

Deutschland setze auf einen präventiven Ansatz, sagte **Christina Stumpp (CDU/CSU)** unter Verweis auf die 2025 erfolgte Umsetzung der europäischen NIS2-Richtlinie. Man müsse aber auch der Realität ins Auge schauen. „Gegen gezielte staatliche Cyberoperationen, hochprofessionelle Kampagnen mit großem Schadenspotenzial reichen präventive Maßnahmen in den eigenen IT-Systemen allein nicht mehr aus“, betonte sie. Deshalb werde mit dem vorliegenden Gesetzentwurf nachgeschärft.

„Wir müssen uns doch ehrlich machen“, forderte die Unionsabgeordnete. Bislang seien den Sicherheitsbehörden angesichts der Vielzahl komplexer Bedrohungen viel zu oft rechtlich die Hände gebunden. Laufe ein Cyberangriff fehlten oft die nötigen Befugnisse, um schnell eingreifen und den Angriff wirksam stoppen zu können, sagte Stumpp.

Die Regelung sieht mehr Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt sowie die Bundespolizei vor. Die Sicherheit und Handlungsfähigkeit von Staat, Wirtschaft und Gesellschaft in einem modernen, hoch technologisierten und digitalisierten Industrieland wie Deutschland beruhen in hohem Maße auf funktionierenden digitalen Prozessen und Infrastrukturen, schreibt die Regierung. Seit Jahren steige jedoch die Zahl von Cyberangriffen durch staatliche und nichtstaatliche Akteure.

Deutschland sei als führende Wirtschaftsnation in Europa verstärkt im Fokus hochprofessioneller Cyberangriffe mit großem Schadenspotenzial. Angesichts der geopolitischen Lage würden zudem auch hybride Bedrohungen zunehmend an Bedeutung gewinnen. „Dieser sicherheitspolitischen Herausforderung begegnet die Bundesregierung, indem sie die Erkennung und Abwehr von Cyberangriffen ausbaut und hierzu wirksame, angemessene und rechtssichere gesetzliche Grundlagen schafft“, heißt es.

Mit der Regelung soll die Aufklärung und die Erkennung konkreter Angriffe und langfristig laufender Angriffskampagnen verbessert werden. Zudem soll die Entdeckung konkreter Vorbereitungshandlungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgebaut werden.

Insbesondere gegen groß angelegte Cyberangriffe mit hohem Schadenspotenzial böten präventive Maßnahmen in den eigenen IT-Systemen allein keinen hinreichenden Schutz, schreibt die Bundesregierung. Es müssten daher für die Polizeien des Bundes und das BSI ergänzend Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen werden, um gravierende Folgeschäden abwenden oder minimieren zu können.

Die Länder bitten in ihrer Stellungnahme (21/7406(Dokument, öffnet ein neues Fenster)) unter anderem darum, die Gesamtbelastung der betroffenen Unternehmen auf ihre Angemessenheit zu prüfen, Bußgelder verhältnismäßig auszugestalten, parallele Melde- und Reportingpflichten „in jedem Fall“ zu vermeiden und die Weitergabe sensibler Daten klar zu begrenzen. Zudem sollen Anforderungen an Auskünfte gegenüber dem Bundesamt für Sicherheit in der Informationstechnik und an sichere Übertragungswege präzisiert werden.

Für Eingriffe des Bundeskriminalamtes in nicht private informationstechnische Systeme verlangt der Bundesrat eine richterliche Anordnung. Nach seiner Auffassung können private und gewerbliche Nutzungen häufig nicht eindeutig voneinander getrennt werden.

Die Bundesregierung lehnt diese Forderungen weitgehend ab. Belastungen und Sanktionsrahmen seien angemessen, die Datenübermittlung hinreichend begrenzt. Überschneidungen mit bestehenden Meldepflichten und unnötige bürokratische Aufwände entstünden nach ihrer Auffassung nicht.

Aufgreifen will sie hingegen den Hinweis, dass bei zwei vorgesehenen Maßnahmen des Bundeskriminalamtes die gerichtliche Zuständigkeit und das Verfahren nicht eindeutig geregelt sind. Dazu kündigt sie für das parlamentarische Verfahren eine Ergänzung des Bundeskriminalamtgesetzes an.

Gegen die Einführung von Hackbacks und offensiver Cyberabwehr, wendet sich die Fraktion Die Linke in ihrem Antrag (21/6653(Dokument, öffnet ein neues Fenster)). Darin fordert die Fraktion die Bundesregierung auf, laufende Gesetzesvorhaben nicht weiter zu betreiben, „die Hackbacks oder vergleichbare Maßnahmen der offensiven Cyberabwehr, gesetzlich verankern würden. Auch soll die Bundesregierung nach dem Willen der Fraktion keine Gesetzesvorhaben weiter betreiben, die dem Bundeskriminalamt (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.

Ebenso sollen dem Antrag zufolge von der Bundesregierung keine Gesetzesvorhaben weiter betrieben werden, „die DNS-Anbieter und Digitale Dienste zur Umleitung von Datenverkehr an das BKA und die Bundespolizei verpflichten könnten,“. Dagegen soll die Bundesregierung laut Vorlage einen Gesetzentwurf vorlegen, der die defensive IT-Sicherheit mit den notwendigen Ressourcen

insbesondere für das Bundesamt für Sicherheit in der Informationstechnik (BSI) stärkt.

In dem Antrag schreibt die Fraktion, dass mit dem Koalitionsvertrag vom Mai 2025 ein Ausbau aktiver Cyberabwehr angekündigt worden sei. Mit dem Gesetzentwurf der Bundesregierung "zur Stärkung der Cybersicherheit,, (21/6585(Dokument, öffnet ein neues Fenster)) solle dieses Vorhaben umgesetzt werden, doch würden die Grenzen des "verfassungsrechtlich Möglichen,, dabei "klar überschritten,,.

Mit dem Entwurf solle für 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, führt die Fraktion weiter aus. Dies bedeute einen massiven Eingriff in informationstechnische Systeme, dem weder ein Richtervorbehalt noch ausreichende parlamentarische Kontrolle als grundrechtssichernde Mechanismen zur Seite gestellt würden. Auch ignoriere der Gesetzentwurf die Möglichkeit, dass Maßnahmen einer "aktiven Cyberabwehr,, auf Eingriffe in fremde staatliche IT-Infrastruktur hinauslaufen könnten. (hau/02.08.2026)

Der **Innenausschuss** hat sich am **Montag, 5. Oktober 2026**, in einer zweistündigen öffentlichen Anhörung mit dem Gesetzentwurf der Bundesregierung zur **Stärkung der Cybersicherheit** (21/6585(Dokument, öffnet ein neues Fenster), 21/7406(Dokument, öffnet ein neues Fenster)) befasst. Die notwendige Stärkung der Cyberabwehr ist dabei unbestritten geblieben. Doch die Bewertungen der Sachverständigen enthielten auch eine ganze Reihe von kritischen Anmerkungen.

Prof. Dr. Dirk Heckmann, Technische Universität München, meinte, der Gesetzentwurf sei im Grundsatz zu begrüßen. Der Staat brauche wirksame Instrumente, um Cyberangriffe frühzeitig zu erkennen und abzuwehren. Der Entwurf schließe hierfür wichtige Regelungslücken. Er machte zugleich gezielten Nachbesserungsbedarf geltend, um die neuen Befugnisse verfassungsrechtlich abzusichern. So müssten der Richtervorbehalt und die qualifizierten Verfahrenssicherungen für jeden verdeckten, manipulierenden oder datenerhebenden Zugriff auf eigengenutzte IT-Systeme gelten – insbesondere dann, wenn auf Opfersysteme eingewirkt werde.

Sven Herpig, Interface, sah bei dem Gesetzentwurf zentrale strukturelle Probleme ungelöst. So beklagte er fragmentierte Zuständigkeiten, inkohärente Eingriffsschwellen, fehlende Governance für intrusive Werkzeuge und eine unzureichende Stärkung von Resilienz. Ohne Koordinierungsmechanismen und Transparenzstandards drohten Effektivitätsverluste und rechtliche Unsicherheiten. So empfahl er, intrusive Eingriffe auf das notwendige Minimum zu beschränken und verfassungsrechtliche Klarheit zu schaffen: Zuständigkeiten zwischen Bund und Ländern müssten eindeutig geregelt werden. Womöglich sei eine Grundgesetzänderung über Befugnisse des Bundeskriminalamts (BKA) erforderlich.

Prof. Dr. Dennis-Kenji Kipker, Cyberintelligence Institute, kritisierte, der Gesetzentwurf gehe in wesentlichen Punkten über das verfassungsrechtlich und sicherheitspolitisch Gebotene hinaus oder lasse erforderliche Sicherungen vermissen. Dies betreffe insbesondere die nur unzureichende richterliche und sonstige unabhängige Kontrolle eingriffsintensiver Maßnahmen, zu weit gefasste Gefahr- und Übermittlungsschwellen sowie unzureichende Vorgaben zum Schutz unbeteiligter Dritter. Hinzu kämen ungeklärte Zuständigkeits- und Koordinationsfragen zwischen Sicherheitsbehörden. Der Entwurf schaffe notwendige Instrumente. Bevor sie aber eingesetzt würden, müsse ebenso klar geregelt sein, wer sie wann einsetzen dürfe, wer darüber wache und wo die Grenzen lägen.

Constanze Kurz, Chaos-Computer-Club, erklärte, das Ziel des Entwurfs, nämlich Maßnahmen für eine Verbesserung der Situation in der IT-Sicherheit zu ergreifen, sei unbedingt unterstützenswert. Doch seien nicht alle dafür gewählten Mittel sinnvoll oder zielführend oder trügen zu

widerstandsfähigen IT-Systemen bei. Insbesondere würden in der Begründung des Entwurfs Risiken und Kollateralschäden von Maßnahmen zur aktiven Cyberabwehr unterbewertet. Vor allem kritisierte sie die Idee des „Hackback“. Die ohnehin desolate Situation in der IT-Sicherheit werde keineswegs verbessert, wenn sich staatliche Stellen im Zurückhacken versuchten und dabei informationstechnische Systeme aktiv veränderten. Die geplanten aktiven Maßnahmen zur Cyberabwehr seien zu invasiv, der IT-Sicherheit insgesamt nicht zuträglich und nicht ausreichend durchdacht.

Holger Münch, Präsident des Bundeskriminalamts, hob hervor, der Gesetzentwurf schließe endlich weitgehend ein seit Jahren bestehendes Defizit. Dem BKA werde eine neue Aufgabe zur Abwehr von Gefahren durch Angriffe auf die IT-Sicherheit übertragen. Flankiert werde diese neue Zuständigkeit durch cyberspezifische Befugnisse, die dem BKA gezielte und verhältnismäßige Maßnahmen zur Gefahrenabwehr erlaubten. Durch die Bündelung von Gefahrenabwehr und Strafverfolgung in einer Hand könne das BKA künftig effektiver und schneller auf die aktuelle Bedrohungslage im Cyberraum reagieren.

Münch sprach von einer gerade entdeckten Lücke im Gesetzgebungsverfahren, als er auf den Drohnen-Vorfall am Flughafen Halle-Leipzig verwies. Die neuen Regelungen griffen immer dann, wenn informationstechnische Systeme betroffen seien, nicht aber, wenn durch Systeme reale Gefahren hervorgerufen würden, wenn also etwa fliegende Computer für Sprengstoffanschläge eingesetzt werden sollten.

Alexander Poitz, Gewerkschaft der Polizei, bewertete den Entwurf als wichtigen Schritt zur Weiterentwicklung der polizeilichen Cyberabwehr. Er begrüßte die Schaffung cyberspezifischer Befugnisse im BKA-Gesetz, die Aufgabenzuweisung für das BKA im Bereich international koordinierter Cyberabwehr, die verbesserte Durchsetzbarkeit von Maßnahmen gegenüber Telekommunikationsanbietern und Anbietern digitaler Dienste sowie die rechtliche Absicherung besonders eingriffsintensiver Maßnahmen durch einen Richtervorbehalt und die Möglichkeit, bei Gefahr im Verzug zunächst selbst tätig zu werden.

Prof. Dr. Haya Schulmann, Goethe-Universität Frankfurt am Main, begrüßte den Gesetzentwurf. Er gebe der aktiven Cyberabwehr die Rechtsgrundlage, die bisher zu einem großen Teil fehle. Maßnahmen im Netz zur Schadensbegrenzung würden ebenso geregelt wie als letztes Mittel der Eingriff in Systeme der Angreifer. Er erweitere zwar die Datenquellen des Bundesamtes für Sicherheit in der Informationstechnik, aber den gesetzlichen Auftrag, daraus ein Lagebild zu erstellen, gebe es nicht. Sie empfehle, diesen Auftrag ins Gesetz zu schreiben und das Eindringen in fremde Systeme stärker zu sichern. (fla/05.10.2026)

<https://www.bundestag.de/dokumente/textarchiv/2026/kw41-pa-inneres-cybersicherheit-1221640>