



Ausschussdrucksache 21(4)221 F
vom 5. Oktober 2026

Schriftliche Stellungnahme

von Dr. Constanze Kurz – Chaos-Computer-Club, Berlin vom
4. Oktober 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung der Cybersicherheit
BT-Drucksache 21/6585



Chaos Computer Club

Stellungnahme

**an den Innenausschuss des Deutschen Bundestags
zum Gesetzentwurf zur Stärkung der Cybersicherheit**

Drucksache 21/6585 vom 22. Juni 2026

Constanze Kurz, Dirk Engling

4. Oktober 2026

Einleitung

Diese Stellungnahme zum Entwurf des Gesetzes zur Stärkung der Cybersicherheit (Drucksache 21/6585) bewertet aus technischer Blickrichtung die neuen Befugnisse, die das BKA, die Bundespolizei und das BSI erhalten soll. Während das Ziel des Entwurfs, nämlich Maßnahmen für eine Verbesserung der Situation in der IT-Sicherheit zu ergreifen, unbedingt unterstützenswert ist, sind nicht alle dafür gewählten Mittel sinnvoll oder zielführend oder tragen zu widerstandsfähigen IT-Systemen bei. Insbesondere werden in der Begründung des Entwurfs Risiken und Kollateralschäden von Maßnahmen zur sog. aktiven Cyberabwehr unterbewertet.

Fähigkeiten zum Gegenschlag und „Hackback“

Bundeskriminalamt (§ 68d) und Bundespolizei (§ 41a) sollen nach dem Gesetzentwurf neue Befugnisse zum Auslesen, zum Löschen oder zum Verändern von Daten in informationstechnischen Systemen erhalten. Die Maßnahmen dürfen mit Wissen der Betroffenen oder auch verdeckt vorgenommen werden.

Zu den kritikwürdigen Vorhaben im Entwurf zählt vor allem die Idee des sog. „Hackback“ im engeren Sinne, das neben anderen Methoden der aktiven Cyberabwehr sowohl dem Bundeskriminalamt als auch der Bundespolizei erlaubt werden soll. Die ohnehin desolate Situation in der IT-Sicherheit wird keineswegs verbessert, wenn sich staatliche Stellen im Zurückhacken versuchen und dabei informationstechnische Systeme aktiv verändern. Denn ein solches Vorgehen ist ein aktiver Angriff auf andere IT-Systeme und gerade keine Verteidigung der eigenen Systeme. Es bedeutet Eskalation, aber keine Verbesserung der eigenen Infrastruktur und Systeme, schon gar keine nachhaltige.

Die für den Erwerb und die Nutzung dieser Fähigkeiten zum Gegenschlag notwendigen Werkzeuge werden absehbar dem durchschnittlichen IT-Sicherheitsniveau einen Bärendienst erweisen. Dies beginnt, wenn dazu bekannt gewordene Sicherheitslücken für eigene Zugriffe offengehalten statt gemeldet und geschlossen werden, inklusive verzögerter Warnungen aufgrund der im Entwurf geplanten Offenbarungsverbote, und endet nicht zuletzt bei der weiteren Erosion des Vertrauens in das BSI, dessen Erkenntnisse künftig auch an den aktuell für erhebliche Befugniserweiterungen vorgesehenen Bundesnachrichtendienst und die Bundeswehr fließen sollen.

Zudem fehlen in Deutschland weiterhin die seit mehr als einem Jahrzehnt überfälligen Regeln zum staatlichen Umgang mit IT-Schwachstellen, die durch Behörden ausgenutzt werden dürfen (Schwachstellen-Management).

Proxy-Systeme

Die Begründung des Entwurfs beschreibt zutreffend Ketten aus Proxy- und VPN-Servern, die von Angreifern in der Praxis genutzt werden. Entsprechend überrascht die nachfolgende, aber irriige Annahme, dass dennoch die Zuschreibung eines Ziels des „Hackback“ schon irgendwie klappen wird und man nicht eine falschen Zwischenstationen hackt. Denn die Zuschreibung (Attribution) eines Angriffs bleibt ein komplexes Problem.

Die Begründung im Entwurf hält die Identifizierung von Angreifern hingegen für „regelmäßig eindeutig möglich“, nämlich anhand von IP-Adressen und Signaturen. Damit ist aber nur ein System identifiziert, nicht aber derjenige, der es faktisch beherrscht. Ob hinter einer IP-Adresse der tatsächliche Angreifer sitzt oder nur ein missbrauchtes Zwischensystem, verraten diese Merkmale gerade nicht.

Praktisch wäre die gefährliche Folge, dass Beamte des BKA oder der Bundespolizei in Systeme direkt eingreifen und sie laut Aussagen des Innenministers „stören und zerstören“ sollen, deren Betreibern eine absichtliche Mitwirkung gar nicht sicher zugeschrieben werden kann. Es drohen daher unerwünschte Seiteneffekte und Fehlsuordnungen.

Denn diese Systeme könnten beispielsweise zu fremder staatlicher Infrastruktur gehören oder missbrauchte Proxy-Systeme kommerzieller Natur sein. Mehr noch: Der Entwurf erlaubt ausdrücklich auch Eingriffe in Opfersysteme und Maßnahmen „wenn Dritte unvermeidbar betroffen werden“. Auch diplomatische Querelen und völkerrechtlich relevante Implikationen wären nicht ausgeschlossen, wenn man dabei etwa Systeme von Verbündeten oder gar von politischen Feinden hackt. Entsprechend drängen sich bei dort verursachten Schäden oder Ausfällen weitere rechtliche Fragen auf.

Im Gegensatz zu Cyberkriminellen, die ein starkes Interesse daran haben, dass ihre gekaperten Opfersysteme nicht auffallen und diese daher möglichst funktionsfähig am Leben halten, sollen BKA und Bundespolizei im Gefahrenfall unter Zeitnot in die Systeme eingreifen dürfen. Im Klartext hieße das: Eine solche Maßnahme verändert Systeme mit unbekannter Konfiguration, darunter möglicherweise auch Systeme, die zum Bereich KRITIS zählen oder etwa Medizin- oder Steuerungstechnik sein können.

Die im Entwurf vorgesehene Rückbaupflicht steht unter dem großzügigen Vorbehalt „soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht“. Wer für Folgeschäden haftet, regelt der Entwurf nicht.

Im Bereich der polizeilichen Gefahrenabwehr muss nicht einmal ein tatsächlicher „Hack“ oder Angriff Auslöser für ein „Hackback“ sein: In der Begründung zu § 41a BPolG steht explizit, dass „in vielen Fällen“ die konkreten Störungen noch gar nicht erkennbar seien. Da in der Gefahrenabwehr bereits Vorbereitungshandlungen genügen und Maßnahmen schon vorgenommen werden können, bevor eine konkrete Störung überhaupt erkennbar ist, rückt das invasive Eingreifen weit ins Vorfeld von Straftaten: Auf den Verdacht hin, ein System könnte im Zusammenhang mit einem bevorstehenden Angriff auf die Sicherheit in der Informationstechnik stehen, dürfen dann Maßnahmen der sog. aktiven Cyberabwehr zum „Aufklären“ ergriffen werden.

Die Begründung des Entwurfs enthält einige Beispielfälle für die Übernahme von C&C-Servern, bei denen die neuen Befugnisse vorstellbar wären. Allerdings erlauben die Befugnisse zahlreiche weitere Szenarien, auch solche von hoher Gefährlichkeit. Denkbar wäre etwa auch ein Gefahrenfall, in dem potentielle Gefährder kryptographische Schlüssel kopiert haben sollen, etwa Funkschlüssel von 50.000 informationstechnischen Systemen, die Fahrzeuge sind. Die Polizei dürfte nach dem Entwurf deren Serverserver übernehmen und den betroffenen Fahrzeugen ein Software-Update aufspielen, das die potentiellen Gefährder aussperren soll. Die Halter oder Fahrer der informationstechnischen Systeme erfahren davon nichts, auch die Hersteller nicht. Welche technische Konfigurationen

(Systemparameter, Werkstattsoftware, Sonderausstattung, Nachrüstungen) in den einzelnen Fahrzeugen stecken, in welchem Land sie gerade fahren, ob es sich dabei vielleicht auch um militärisch genutzte oder Diplomaten-Fahrzeuge handelt, all das kann die Polizei in diesem Beispielfall nicht wissen. Verursachen die Modifikationen Ausfälle oder gar verheerende Unfälle, ist die Haftung für Schäden komplett ungeklärt.

Evaluierung

Dem Gesetzentwurf mangelt es an einer Vorschrift zur Evaluierung der neuartigen Befugnisse, deren Wirkung im Sinne des Zieles des Entwurfs nicht belegt und teilweise nicht einmal wahrscheinlich ist. Gerade bei neuartigen und eingriffsintensiven Befugnissen, die ohne Befristung eingeführt werden sollen, verlangt der Nationale Normenkontrollrat diese Evaluierung jedoch. Sie ist auch sachlich zu befürworten, um Nutzen und Risiken sinnvoll abwägen zu können. Daher wäre zudem eine umfassende Berichtspflicht sinnvoll.

Als Begründung, warum auf die Evaluierung verzichtet werden könne, wird angegeben, dass die neuen Regelungen an bestehende Rechtsstrukturen anknüpfen und die Auswirkungen „im Wesentlichen prognostizierbar“ seien. Beides ist ausgesprochen fragwürdig und für die Prognostizierbarkeit technisch wenig wahrscheinlich.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen

Die geplanten Maßnahmen greifen unzweifelhaft in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen ein und wären daher mit engen Grenzen zu versehen. Das Bundesverfassungsgericht hat im Juni 2021 zudem in einem Beschluss zum Umgang von Polizeibehörden mit Sicherheitslücken in Programmen oder sonstigen informationstechnischen Systemen ausgeführt,¹ dass die staatliche Schutzpflicht eine gesetzliche Regelung verlangt, die den Zielkonflikt zwischen dem Schutz von IT-Systemen und dem Offenhalten unbekannter Sicherheitslücken für behördliche Zwecke grundrechtskonform auflöst. Der Entwurf greift diesen Auftrag nicht ausreichend auf, obwohl er die Ausnutzung von Lücken vorsieht.

Dabei ist noch nicht einmal die Erforderlichkeit der geplanten Maßnahmen ausreichend dargelegt: So wird in der Begründung der Emotet-Fall angeführt, also eine Botnet-Bereinigung, die das BKA im Jahr 2021 erfolgreich durchgeführt hat. Die Begründung erklärt allerdings nicht, welche gesetzlichen Befugnisse tatsächlich fehlten, da der Emotet-Fall ja zu bewältigen war.

Der Entwurf begründet die Notwendigkeit der neuen Befugnisse mit einem erheblichen Bedrohungsszenario, auch mit von Staaten gesteuerten „hybriden“ Großangriffen. Dem widerspricht jedoch die tatsächliche Definition eines „Angriffs auf die Sicherheit in der Informationstechnik“, die bei alltäglichen IT-Angriffen ansetzt: Ein solcher Angriff liegt

¹ BVerfG, Beschluss des Ersten Senats, 1 BvR 2771/18, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html vom 8. Juni 2021, abgerufen am 3. Oktober 2026.

demnach bei jeder konkreten Gefahr einer Straftat nach §§ 202a–202d, 263a, 303a, 303b StGB vor. Bei der Bundespolizei ist das konkret der Computerbetrug (§ 263a), Phishing und Vorbereitungshandlungen (§ 202c) und Datenhehlerei (§ 202d).

Die bereits erfolgte schrittweise Ausweitung bei den Befugnissen zum Staatstrojaner-Einsatz als sog. Quellen-TKÜ und als sog. Online-Durchsuchung bei den Polizeien zeigt, dass auch eine zukünftige Ergänzung der Befugnisse zur aktiven Cyberabwehr nicht unrealistisch erscheint. Das gilt vor allem, weil eine Evaluation nicht vorgesehen ist.

Von den geplanten Maßnahmen zur aktiven Cyberabwehr ist abzusehen, da sie intensiv in Grundrechte eingreifen. Sie werden zudem absehbar gefährliche Nebenwirkungen haben und lassen weitreichende Eingriffe in Systeme von Opfern und unbeteiligten Dritten zu. Es mangelt außerdem weitgehend an der notwendigen richterlichen Kontrolle. Im Bereich der Strafverfolgung müssen solche Eingriffe in informationstechnische Systeme aus gutem Grunde strengen Vorgaben genügen und sind selbstverständlich durch einen Richter zu prüfen, aber in der Gefahrenabwehr bei „Cybergefahren“ sollen sie nun weitgehend ohne Richtervorbehalt und ohne klare gesetzliche Schranken bei unangemessen trivialen Anlässen aus dem digitalen Waffenschrank geholt werden.

Untersagungen

Sowohl das BKA (§ 68b) als auch die Bundespolizei (§ 41a) sollen nach dem Gesetzentwurf als neue aktive Eingriffsbefugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik („Cybergefahr“) auch eine Untersagung des Betriebs von informationstechnischen Systemen aussprechen dürfen, wenn die Gefahr von diesen Systemen ausgeht. Angenommen wird in der Begründung, dass beim BKA pro Jahr etwa 300 Anwendungsfälle zu erwarten sind, bei der Bundespolizei etwa 30. Worauf diese Zahlen gründen, bleibt offen. Laut Begründung soll das BKA nur in eng begrenzten, schwerwiegenden Fällen zuständig sein. Mit zehnmal so vielen Untersagungen wie die Bundespolizei rechnet es trotzdem.

Diese Untersagung soll sich an Anbieter von Telekommunikationsdiensten nach dem Telekommunikationsgesetz sowie an Anbieter digitaler Dienste richten. Die Untersagung kann sich aber ausdrücklich auch an Privatpersonen und Unternehmen jeder Art richten. Praktisch zielt die Befugnis wohl auf Hoster und Rechenzentren, deren Kunden Systeme missbrauchen. Im Gesetzentwurf selbst ist aber keine Beschränkung auf bestimmte informationstechnische Systeme festgelegt. Daher ist die faktische Handlungsmacht aufgrund dieser Befugnis größer, als es in den Beispielen der Entwurfsbegründung anklingt.

Diese neue Befugnis ist weitreichend und belastet zahlreiche Dritte. Übertragen in ein Beispiel der analogen Welt hieße das: Im Falle, dass ein Gast in seinem Zimmer Straftaten planen soll oder ein potentieller Gefährder ein Zimmer ohne Wissen des Hoteliers nutzt, darf die Polizei daraufhin die Schließung des Hotels anordnen, ohne eine Genehmigung durch einen Richter einholen zu müssen und ohne eine gesetzliche Höchstdauer. Ob nur das Zimmer oder das ganze Hotel betroffen sind, legt das Gesetz nicht fest. Öffnet der Hotelier trotzdem, droht ihm ein Bußgeld bis zu 500.000 Euro. Den Hotelgästen, die vor verschlossener Tür stehen, darf er unter Umständen nicht einmal sagen, warum.

Automatisierte Übermittlungen an das BSI

Mit der geplanten Änderung des § 31 Abs. 2 BSIG sollen die KRITIS-Betreiber verpflichtet werden, Systeme zur Angriffserkennung direkt an die Systeme des BSI anzubinden. Das ist eine fundamentale Veränderung im Vergleich zu der vorherigen Regelung, nach der Systeme zur Angriffserkennung nur verpflichtend auf dem Stand der Technik zu betreiben sind. Allerdings steht die Anbindung an das BSI unter einem Wirtschaftlichkeitsvorbehalt.

Nach dem Entwurf ist eine kontinuierliche und automatisierte Übermittlung über eine direkte Schnittstelle vorgesehen, die in der Begründung mit einem Minutentakt angegeben ist. Übermittelt werden sollen die Verfügbarkeitsindikatoren der wesentlichen Systeme und Betriebsdaten.

Welche Daten in welchem Umfang fließen, legt allein das BSI per technischer Richtlinie fest (§ 31 Abs. 6). Der Gesetzgeber gibt dem Umfang damit keine Obergrenze vor. Daher stellt sich zunächst die praktische Frage, ob das BSI mit den veranschlagten 9 Stellen rund 2.100 angebundene Anlagen (Erfüllungsaufwand Nr. 4.2.7) überhaupt auswerten kann. Das jedoch hängt maßgeblich von den technischen Details der Übermittlung ab.

Die im Entwurf angesprochenen „Systeme zur Angriffserkennung“ können in der Praxis SIEMs (Security Information and Event Management) sein, die typischerweise Dutzende bis Hunderte Events pro Tag auswerfen, oder auch Intrusion Detection Systems (FW, Proxy usw.), die Dutzende bis Hunderte Events pro Minute oder Sekunde aufzeichnen. Wenn das BSI im Detail festlegt, was geliefert werden muss, dann können sie damit das übermittelte Volumen steuern.

Unabhängig von diesen noch ungeklärten Details werden in solchen Systemen auch in großer Zahl bloße Verdachtsfälle für IT-Angriffe aufgezeichnet. Vor allem aber wären in den übermittelten Daten zweifelsohne zahlreiche klar personenbezogene Daten, die dann massenhaft an das BSI ausgeleitet würden.

Das Ziel hinter dem Vorhaben, nämlich beim BSI alle Hinweise auf IT-Angriffsversuche (IOC Sharing) über alle KRITIS hinweg zu bündeln und ein Lagebild zu bekommen, ist im Grundsatz zwar unterstützenswert und kann einen Mehrwert liefern. Allerdings könnte das BSI dafür MISP (Malware Information Sharing Platform) heute schon nutzen. Jedoch schreibt das BSI bis heute nicht einmal den Konsum von ihrem MISP vor.

Wird die Anbindung umgesetzt, entsteht beim BSI eine unverhältnismäßig große Datensammlung, inkl. zahlreicher personenbezogener Daten. Die Schnittstelle zum BSI und damit eine offene Verbindung zu Dritten nach außen birgt zudem die Gefahr weiterer Angriffspunkte. Die im Entwurf vorgesehene zentrale Bündelung von KRITIS-Indikatoren beim BSI würde durch die neue Meldepflicht also ein neues Angriffsziel schaffen. Die Sicherheitsanforderungen an die Übermittlung lässt der Entwurf offen oder überlässt sie weitgehend untergesetzlichen Festlegungen.

Fazit

Die geplanten aktiven Maßnahmen zur Cyberabwehr sind zu invasiv, der IT-Sicherheit insgesamt nicht zuträglich und nicht ausreichend durchdacht. Wir empfehlen, sie zu streichen.

Der nach wie vor beklagenswerte Zustand vieler und vor allem der weitverbreiteten IT-Produkte und IT-Systeme in Wirtschaft und Verwaltung ist das eigentliche Problem. Sonst bräuhete es die im Entwurf vorgeschlagenen Maßnahmen in diesem Umfang nicht. Die geplanten eingriffsintensiven Maßnahmen der aktiven Cyberabwehr sind im Gegensatz zu Maßnahmen, die defensiv oder tatsächlich präventiv Angriffe verhindern, nicht nachhaltig und tragen damit gar nicht oder nur sehr kurzfristig zur Verbesserung der Resilienz gegen Angriffe bei.

Schon deswegen sollten offensive Gegenmaßnahmen auf ein Minimum beschränkt sein und nachhaltigen und langfristig effektiven Methoden zum Schutz der eigenen IT-Systeme der Vorzug gegeben werden. Das heißt zugleich, weniger invasive Methoden mit weniger oder bestenfalls gar keinen Nebenwirkungen vorzuziehen. Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen sind nicht nur in der Strafverfolgung, sondern auch in der Gefahrenabwehr rigorose Grenzen zu setzen.

Hält der Gesetzgeber an den Befugnissen fest, sind mindestens folgende Korrekturen erforderlich:

- Richtervorbehalt für alle Maßnahmen, die in fremde Systeme eingreifen oder Datenverkehr aufzeichnen, ob privates System oder nicht,
- gesetzliche Regelungen zum Umgang mit IT-Sicherheitslücken, die den Vorgaben des Bundesverfassungsgerichts von 2021 genügen, inkl. Schwachstellen-Management,
- eine Befristung der neuen Befugnisse sowie unabhängige Evaluierung,
- gesetzlich festgelegte Sicherheitsanforderungen für die Datenausleitung an das BSI sowie eine Höchstdauer für Untersagungen des Betriebs.

Diese Anforderungen erscheinen noch dringender, da mit den parallel geplanten Reformen auch BND und Bundesamt für Verfassungsschutz aktive Eingriffsbefugnisse erhalten sollen. Nötig ist deshalb eine „Eingriffsgesamtrechnung“ als Überblick zur Proliferation der staatlichen Eingriffsmöglichkeiten in informationstechnische Systeme.