



Ausschussdrucksache 21(4)221 D
vom 2. Oktober 2026

Schriftliche Stellungnahme

von Holger Münch, Präsident des Bundeskriminalamts, Wiesbaden
vom 2. Oktober 2026

zu dem

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



Bundeskriminalamt • 65173 Wiesbaden

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

Am Treptower Park 5-8
12435 Berlin

Zentrale Postanschrift:
65173 Wiesbaden

Tel. +49 611 55-0

Leitungsstab 4

www.bka.de

Anhörung zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit am 05.10.2026

Berlin, 02.10.2026
Seite 1 von 8

Vorbemerkung

Cybersicherheit ist ein wesentlicher Baustein der Funktionsfähigkeit des Gemeinwesens. Angriffe auf Krankenhäuser, kommunale Verwaltungen, politische Institutionen, Energieversorger und Verkehrsbetriebe treffen nicht nur Serverräume, sondern ganz konkret das Funktionieren unserer Gesellschaft bis hin zur lebensnotwendigen Versorgung von Menschen. Die Bedrohungslage hat sich dabei nicht nur quantitativ verschärft: Angriffe erfolgen zunehmend professionell organisiert, arbeitsteilig und in Teilen staatlich gesteuert – nicht zuletzt auch aufgrund der Verschärfung der geopolitischen Lage. Der Branchenverband Bitkom beziffert den wirtschaftlichen Schaden für Deutschland durch Cyberattacken allein für das Jahr 2026 auf bis zu 206 Milliarden Euro¹.

Mit dem nunmehr vorliegenden Entwurf des Gesetzes zur Stärkung der Cybersicherheit kann nach Einschätzung des Bundeskriminalamts (BKA) endlich eine seit Jahren bestehendes Defizit weitgehend geschlossen werden. Dies betrifft sowohl die Aufgabenzuweisung zur polizeilichen Gefahrenabwehr im Cyberraum als auch die zur Umsetzung erforderlichen cyberspezifischen Befugnisse. Das BKA begrüßt es sehr, hierfür das notwendige Instrumentarium zu erhalten.

¹ Bitkom-Studienbericht Wirtschaftsschutz 2026



Seite 2 von 8

Ausgangslage

Bereits im Jahr 2021 gelang deutschen Sicherheitsbehörden einer der seinerzeit bedeutendsten Schläge gegen die internationale Cyberkriminalität: Die Generalstaatsanwaltschaft Frankfurt am Main -Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)- und das BKA übernahmen gemeinsam mit Partnerbehörden aus sieben Staaten sowie mit Unterstützung von Europol und Eurojust die technische Infrastruktur der Schadsoftware „Emotet“. Dabei wurden verschiedene Einzelmaßnahmen umgesetzt.

- Die Serverinfrastruktur der Täterseite wurde übernommen,
- über ein Update wurden Kommunikationsparameter der Schadsoftware so verändert, dass infizierte Systeme nur noch mit einer behördlich kontrollierten Infrastruktur kommunizieren konnten,
- das Schadprogramm wurde auf den Opfersystemen in Quarantäne verschoben und
- die festgestellten IP-Adressen von infizierten Nutzern wurden vom BKA an das Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelt, damit dieses über die Provider die betroffenen Kundinnen und Kunden informieren und warnen konnten.

„Emotet“ galt als eine der gefährlichsten Schadsoftware weltweit und hat auch in Deutschland neben Computern zehntausender Privatpersonen eine hohe Anzahl von IT-Systemen von Unternehmen, Behörden und Institutionen infiziert. Der Fall war aus Sicht des BKA ein Erfolg. Bei näherer Betrachtung legt er jedoch offen, woran es fehlte und auch heute noch fehlt:

Rechtlich war der Emotet-Takedown eine strafprozessuale Maßnahme im Rahmen eines Ermittlungsverfahrens. Erforderlich waren aber zum damaligen Zeitpunkt bereits Maßnahmen der polizeilichen Gefahrenabwehr, da es darum ging, ein laufendes Botnetz handlungsunfähig zu machen und tausende Opfersysteme zu bereinigen. Um im Sinne der Cybersicherheit überhaupt handlungsfähig zu sein, musste das Strafprozessrecht so weit wie möglich ausgelegt werden – und dennoch verblieb eine erhebliche Lücke: Ein durch die Täter programmierter Deinstallationsbefehl von Emotet durfte nicht genutzt werden.

Dass in diesem Verfahren gefahrenabwehrende Maßnahmen über das Strafverfahrensrecht abgewickelt werden mussten, ist kein Einzelfall, sondern das Symptom einer doppelten Lücke. Die erste Lücke betrifft Zuständigkeiten (Aufgaben). Gefahrenabwehr ist nach der Kompetenzordnung des Grundgesetzes grundsätzlich Sache der Länder. Diese zu gänzlich „analogen“ Zeiten entwickelte Kompetenzzuweisung trägt im Cyberraum aber nicht mehr.



Seite 3 von 8

Gefahren treten zum annähernd selben Zeitpunkt mindestens länderübergreifend, wenn nicht sogar das ganze Bundesgebiet betreffend, ein und sie haben in nahezu allen Fällen eine internationale Komponente. Das bisherige Vorgehen aus der analogen Welt ist deshalb nur bedingt anwendbar. Die Polizeien der Länder sind zuständig, aber weder territorial noch rechtlich in der Lage, Gefahren mit geeigneten Mitteln abzuwehren.

Praktisch bedeutet dies auch noch heute: Das Bundeskriminalamt kann einen laufenden Angriff erkennen und dokumentieren, gefahrenabwehrend beenden darf es ihn jedoch nicht. Gleichzeitig obliegt dann aber dem BKA die Strafverfolgung eben dieses Sachverhalts. Und genau dieser Zustand ist spätestens in der aktuellen Zeit aus sicherheitspolitischer Perspektive nicht weiter hinnehmbar.

Daher bedarf es rechtlicher Anpassungen, um der geänderten Situation an zentraler Stelle besser begegnen zu können und die Bundesrepublik auch im digitalen Zeitalter handlungsfähig für Gefahrenlagen im digitalen Raum zu machen. Hierfür soll das BKA eine neue Aufgabe erhalten.

Die zweite Lücke betrifft die derzeit bestehenden Befugnisnormen. Es fehlen spezifische Befugnisse für die zielgerichtete Abwehr von Gefahren im Cyberraum. Das BKA ist zwar technisch in der Lage, gefahrenabwehrende Maßnahmen, wie das Umleiten von gefahrengegenständlichem Datenverkehr, Maßnahmen gegen von Angreifern genutzte Server oder zum Schutz von Opfersystemen umzusetzen. Die bestehenden Befugnisse im BKAG lassen die vorgenannten Maßnahmen allerdings rechtlich derzeit nicht zu. Auch die Generalklausel des § 38 BKAG kann aufgrund bereits erfolgter richterlicher Entscheidungen hierfür nicht fortgesetzt herangezogen werden. Somit fehlen die nunmehr im Entwurf angedachten cyberspezifischen Befugnisnormen, damit technische Maßnahmen wie beispielsweise der Einsatz eines bereits durch die Täter in die Schadsoftware „Emotet“ eingebauten Deinstallationsbefehls auch rechtskonform erfolgen kann.

Neue Aufgabennorm § 3a BKAG-E

Der neue § 3a BKAG-E weist dem BKA eine neue, eng umgrenzte Aufgabe im Bereich der Cyberabwehr zu, um die geschilderte Lücke zu schließen. Die neue Aufgabe umfasst drei Fallgruppen:

- Cybergefahren, die nur in internationaler Zusammenarbeit abgewehrt werden können,
- Cybergefahren, die die Funktionsfähigkeit von Bundesbehörden und -einrichtungen beeinträchtigen können sowie



Seite 4 von 8

- Cybergefahren mit besonderer außen- oder sicherheitspolitischer Relevanz.

Dem BKA wird also **nicht** die allgemeine Zuständigkeit für die polizeiliche Abwehr von Cyberangriffen übertragen – auch nicht in den Fällen, in denen diese, wie im Cyberraum üblich, internationale Bezüge aufweisen. Es handelt sich um eine punktuelle, klar abgegrenzte Aufgabenerweiterung.

Die erste Alternative ermöglicht dem BKA die Abwehr **schwerwiegender Cyberangriffe zu übernehmen, deren Abwehr nur gemeinsam mit den zuständigen Stellen anderer Staaten** umgesetzt werden kann. Als schwerwiegend gelten dabei Cyberbedrohungen, die sich gegen die innere oder äußere Sicherheit der Bundesrepublik oder gegen die genannten Behörden und Einrichtungen richten, etwa Angriffe auf die Energie-, Wasser-, Gesundheits- oder Lebensmittelversorgung. Erfasst sind auch Angriffe auf die Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Zahl von Personen – insbesondere Fälle, in denen mehrere Tausend IT-Systeme infiziert und zu einem sog. „Botnetz“ verbunden sind. Diese Kriterien orientieren sich an der bestehenden Zuständigkeit des BKA für die Strafverfolgung im Bereich Cybercrime (§ 4 Abs. 1 Nr. 5 BKAG). Die Aufgabe adressiert koordinierte internationale Polizeioperationen – etwa gegen Botnetze: Netzwerke aus tausenden kompromittierten Geräten, die beispielsweise für Spam-Versand, DDoS²-Angriffe oder Datendiebstahl missbraucht werden. Wegen ihrer dezentralen Struktur lassen sich solche Netzwerke meist nur durch zeitgleiches Vorgehen mehrerer Staaten wirksam bekämpfen; ein isoliertes nationales Vorgehen würde durch die im Ausland verbliebene Infrastruktur unterlaufen und durch die kriminellen Akteure kompensiert. Da die Teilnahme an derartigen Operationen etablierte internationale Vernetzung voraussetzt und typischerweise nur einer nationalen Behörde je Staat vorbehalten ist, übernimmt diese Rolle für Deutschland das BKA – analog zu der schon bestehenden Zuständigkeit im Bereich der Strafverfolgung Cybercrime. Alle übrigen Fälle, in denen keine schwerwiegende Gefahr vorliegt und in denen nicht das Erfordernis internationaler Kooperation besteht – verbleiben in der allgemeinen Gefahrenabwehrzuständigkeit der Bundesländer.

Die zweite Alternative begründet eine Zuständigkeit des BKA für die **Abwehr von Cyberangriffen, die die Funktionsfähigkeit von Behörden und Einrichtungen des Bundes gefährden**. Die Beschränkung auf die Funktionsfähigkeit trägt der Gesetzgebungskompetenz

² DDoS: Distributed Denial-of-Service



Seite 5 von 8

des Bundes Rechnung: Nicht jede Cybergefahr für eine Bundesbehörde begründet eine Zuständigkeit des BKA, sondern nur solche, die die Funktionsfähigkeit der betroffenen Stelle tatsächlich bedroht.

Die dritte Alternative erlaubt dem BKA, Maßnahmen zur Abwehr von Cyberangriffen umzusetzen, wenn sich die Angriffe **ihrer Art nach oder wegen der zur Abwehr erforderlichen Maßnahmen auf die Stellung Deutschlands in der Staatengemeinschaft oder auf die Verteidigung auswirken kann**. Gemeint sind insbesondere Maßnahmen, die von Deutschland aus IT-Systeme im Ausland betreffen, etwa das Verändern oder Löschen von Daten auf Systemen der Angreifer. Die hierfür erforderlichen außen- und sicherheitspolitischen Lageeinschätzungen und Abwägungen kann nur der Bund leisten, da nur er kurzfristig über die notwendigen Informationen verfügt und aus seiner Zuständigkeit für auswärtige Angelegenheiten heraus mögliche außenpolitische Folgen bewerten kann. Relevant sind etwa Fälle, in denen ein anderer Staat Deutschland um Unterstützung bittet, oder Angriffe, die von einer fremden Macht ausgehen oder von dieser unterstützt werden. Eine Betroffenheit der Verteidigung kann beispielsweise bei einem gewichtigen Angriff auf einen Rüstungshersteller vorliegen.

Der Anwendungsbereich der neuen Aufgabennorm ist klar abgegrenzt, indem diese zum einen nur Cybergefahren im engeren Sinne erfasst, also Angriffe auf IT-Systeme selbst; Cybergefahren im weiteren Sinne – etwa Sexualdelikte oder Drogenhandel im Internet – fallen nicht darunter. Zum anderen bleibt die allgemeine Zuständigkeit der Länder für die Gefahrenabwehr im Cyberraum unberührt, einschließlich der Cyberabwehr im Zusammenhang mit lebenswichtigen Einrichtungen, soweit keine Bundesbehörde betroffen ist oder keine internationale Koordination erforderlich wird.

Befugnisse

Zur wirksamen Wahrnehmung der neuen Aufgabe erhält das BKA neben den bereits bestehenden klassischen Befugnissen (z.B. Sicherstellung von Servern, Telekommunikationsüberwachung) cyberspezifische Befugnisse zur Untersagung des Betriebs informationstechnischer Systeme, zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr sowie zum Auslesen, Löschen und Verändern gefahrgegenständlicher Daten in informationstechnischen Systemen.

In bestimmten Konstellationen genügt bereits die **Untersagung des Betriebs eines informationstechnischen Systems**, um eine Cybergefahr wirksam abzuwehren. § 68b BKAG-E



Seite 6 von 8

schafft hierfür die entsprechende Befugnis. Möglich ist dabei nicht nur die vollständige, sondern, als milderes Mittel, auch die teilweise Untersagung oder Einschränkung des Betriebs. Die Norm dient insbesondere dem Zweck, durch Angreifer genutzte Infrastrukturen sowie infizierte Systeme, von denen eine Gefahr ausgeht, abschalten zu lassen. Praktisch bedeutsam ist dies etwa für die Deaktivierung infizierter „Bots“ oder sog. „Command-and-Control-Server“, über die Angriffe gesteuert und koordiniert werden. Die Deaktivierung erfolgt dabei nicht unmittelbar durch das BKA selbst, sondern im Wege der Verpflichtung oder Inanspruchnahme der jeweils zuständigen Diensteanbieter. Als typische Adressaten kommen Anbieter von Telekommunikationsdiensten nach dem Telekommunikationsgesetz (TKG) sowie Anbieter digitaler Dienste nach dem TDDDG³ in Betracht.

Die Regelung **§ 68c BKAG-E** ermöglicht es dem BKA den **Datenverkehr einzuschränken, zu unterbinden oder umzuleiten**. Wird Datenverkehr einer Domain oder IP-Adresse auf eine durch das BKA vorgegebene Zieladresse umgeleitet, darf dieser auch aufgezeichnet werden. Bei dem in Rede stehenden Datenverkehr handelt es sich in der Regel um Steuerungsinformationen der Schadprogramme sowie um IP-Adressen oder andere Internetkennungen der betroffenen, zu einem Botnetz zusammengeschlossenen Systeme. Ein typischer Anwendungsfall ist die Bereinigung von mit Schadsoftware infizierten Computersystemen, die zu einem Botnetz zusammengeschlossen wurden. Nachdem die Domain des zugehörigen Steuerungsservers (Command-&-Control-Server) sichergestellt wurde, kann der schädliche Datenverkehr auf ein polizeilich kontrolliertes System – ein sog. „Sinkhole“ – umgeleitet werden.

Auch bei Angriffen mit erkennbaren Mustern kann der zugehörige Datenverkehr bei Telekommunikationsanbietern (z. B. Access-Providern) umgeleitet werden, um ihn später zu verwerfen oder zu Analysezwecken an eine vom BKA vorgegebene Adresse weiterzuleiten. Bei DDoS-Angriffen kann zudem verhindert werden, dass Angriffsdatenverkehr überhaupt erst erzeugt wird.

Die Vorschrift **§ 68d BKAG-E** erlaubt es dem BKA, **bestimmte für die Gefahr relevante Daten in informationstechnischen Systemen auszulesen, zu verändern oder zu löschen** –, jedoch nur wenn in Beachtung des Verhältnismäßigkeitsgrundsatzes kein milderes gleich geeignetes Mittel zur Abwehr der Cybergefahr zur Verfügung steht. Die Befugnis räumt es dem BKA ein, mit

³ Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten



Seite 7 von 8

technischen Mitteln in das System eines Angreifers einzugreifen, von dem ein Cyberangriff ausgeht, um es unter Ausschluss des eigentlich Berechtigten zu steuern oder abzuschalten.

Die **Übernahme oder Steuerung eines Command-&-Control-Servers** kann z.B. genutzt werden, um den in der Schadsoftware enthaltenen Deinstallationsbefehl („Kill-Switch“, vgl. Emotet) auszulösen oder ein Update mit geänderten Kommunikationsparametern an infizierte Systeme zu senden. Diese kommunizieren dann nicht mehr mit der technischen Infrastruktur des Angreifers, sondern mit einer vom BKA vorgegebenen Zieladresse („Sinkhole“). Dabei dürfen nur solche Daten von den infizierten Systemen an das BKA ausgeleitet werden, die für die Identifizierung und Bereinigung der betroffenen Systeme zwingend erforderlich sind. Diese werden anschließend vom BKA dem BSI mit dem Ziel der Verteilung an die zuständigen Provider und Benachrichtigung der Betroffenen übermittelt.

Auch direkte Veränderungen an einem Angreifersystem – etwa an dort laufenden Skripten – kann das BKA vornehmen, um **einen Angriff unmittelbar zu stoppen**. Läuft beispielsweise ein DDoS-Angriff über einen Server, dessen Anbieter das BKA nicht zur Abschaltung verpflichten kann, darf das BKA mit technischen Mitteln auf den Server zugreifen und die notwendigen Änderungen vornehmen.

Die Befugnis erlaubt zudem **begrenzte Eingriffe in Systeme Geschädigter**, von denen im Rahmen eines Angriffs selbst eine Gefahr ausgeht. So darf das BKA Konfigurationsdaten der Schadsoftware verändern oder löschen. Verfügt eine Schadsoftware – wie z. B. Emotet – über einen eingebauten Deinstallationsbefehl, kann das BKA diesen an betroffene Geräte senden.

Fazit

Der vorliegende Gesetzentwurf überträgt dem BKA mit § 3a BKAG-E eine neue Aufgabe zur Abwehr von Gefahren durch Angriffe auf die IT-Sicherheit. Flankiert wird diese neue Zuständigkeit durch cyberspezifische Befugnisse, die dem BKA gezielte und verhältnismäßige Maßnahmen zur Gefahrenabwehr erlauben. Durch die Bündelung von Gefahrenabwehr und Strafverfolgung in einer Hand kann das BKA künftig effektiver und schneller auf die aktuelle Bedrohungslage im Cyberraum reagieren. Dies entspricht auch der Erwartungshaltung der Bundesländer, welche sich eine klar definierte Bundeszuständigkeit bei der Abwehr von polizeilichen Cybergefahren wünschen.



Seite 8 von 8

Ergänzend dazu sieht der Gesetzentwurf vor, dass auch die Bundespolizei und das BSI Befugnisse für die Abwehr von Cybergefahren in ihrem spezifischen polizeilichen bzw. ordnungsbehördlichen Zuständigkeitsbereich erhalten sollen.

Der Gesetzentwurf stellt damit einen wesentlichen und dringend notwendigen Schritt zur Stärkung der aktiven Cybersicherheit auf Bundesebene in Deutschland dar und ergänzt die bestehenden Möglichkeiten der genannten Behörden, um gemeinsam Gefahren im Cyberraum abzuwehren.

Abschließend möchte das BKA aufgrund von aktuellen Lageentwicklungen darauf hinweisen, dass die Sicherheitsbehörden des Bundes und der Länder in der vergangenen Zeit verstärkt feststellen, dass staatliche Akteure zur Begehung von Straftaten mit bundesweitem Charakter (wie bspw. der Herbeiführung von Sprengstoffexplosionen an verschiedenen Orten im Bundesgebiet) vermehrt informationstechnische Systeme verwenden.

Aufgrund der sich ergebenden Gefahrenlage nach § 5 BKAG (Abwehr von Gefahren des internationalen Terrorismus) ergibt sich aus Sicht des BKA aktueller rechtlicher Anpassungsbedarf, welchen BKA-Präsident Münch in der Anhörung am 05.10.2026 gerne den Abgeordneten des Innenausschusses im Deutschen Bundestag näher erläutern würde.