Deutscher Bundestag **Drucksache 21/9159**

21. Wahlperiode 11.11.2026

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

a) zu dem Gesetzentwurf der Bundesregierung
– Drucksachen 21/6585, 21/7406 –

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

b) zu dem Antrag der Abgeordneten Donata Vogtschmidt, Clara Bünger, Anne-Mieke Bremer, weiterer Abgeordneter und der Fraktion Die Linke
– Drucksache 21/6653 –

Gegen die Einführung von Hackbacks und offensiver Cyberabwehr

A. Problem

Zu Buchstabe a

Mit dem Gesetzesentwurf beabsichtigt die Bundesregierung, die Cybersicherheit in Deutschland angesichts zunehmender und komplexer Cyberangriffe sowie hybrider Bedrohungen zu stärken. Die Fähigkeiten zur frühzeitigen Erkennung und der Abwehr von Cyberangriffen sollen ausgebaut und hierzu wirksame, angemessene und rechtsklare gesetzliche Grundlagen geschaffen werden. Insbesondere sollen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeien des Bundes zusätzliche Befugnisse zur Unterbindung schwerwiegender Cyberangriffe erhalten, um kritische Infrastrukturen, wichtige Unternehmen und staatliche Einrichtungen besser zu schützen und gravierende Schäden abzuwenden.

Zu Buchstabe b

Die Fraktion Die Linke lehnt offensive Cyberabwehrmaßnahmen, insbesondere sogenannte „Hackbacks“, und weitreichende Eingriffsbefugnisse für das BKA und die Bundespolizei ab. Stattdessen fordert sie die Bundesregierung auf, einen

Gesetzesentwurf vorzulegen, der die defensive Cybersicherheit stärkt, das BSI mit zusätzlichen Befugnissen und Ressourcen ausstattet sowie die Gewährleistung des Grundrechts- und Datenschutzes sowie des Völkerrechts sicherstellt.

B. Lösung

Zu Buchstabe a

Der Innenausschuss empfiehlt mit dieser Beschlussempfehlung, den Gesetzentwurf im Wesentlichen um folgende Maßnahmen abzuändern und zu ergänzen:

– Aufnahme verdeutlichender Aspekte zu dem Verhältnismäßigkeitsgrundsatz im BKAG und BPOLG.

– Erweiterung der neuen cyberspezifischen Befugnisse des BKA auf realweltliche Gefahren (z.B. Steuerungsgeräte von Drohnen).

– Einfügung einer Evaluierungsklausel für die durch das Gesetz eingeführten oder geänderten Regelungen.

– Einfügung (rechtsförmlicher) Korrekturen sowie von Folgeänderungen im Zusammenhang mit anderen Gesetzgebungsvorhaben.

Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke.

Annahme einer Entschließung mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktionen AfD und Die Linke.

Zu Buchstabe b

Ablehnung des Antrags auf Drucksache 21/6653 mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion Die Linke bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN.

C. Alternativen

Ablehnung des Gesetzentwurfs zu Buchstabe a und/oder Annahme des Antrags zu Buchstabe b.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Für das BKA entsteht ein Bedarf von 49 Beschäftigten im höheren Dienst und 215 im gehobenen Dienst und damit korrespondierend ein jährlicher finanzieller Bedarf i. H. v. 33,94 Millionen Euro. Zudem entsteht ein jährlicher Sachmittelbedarf von 5 Millionen Euro für die Beschaffung von Hard- und Softwareprodukten sowie Betriebs-, Wartungs- und Pflegekosten der technischen Umgebung.

Beim BSI entsteht für die Wahrnehmung der durch dieses Gesetz zugewiesenen Aufgaben ein jährlicher Mehrbedarf aufwachsend bis zum Jahr 2030 in Höhe von rund 3 Millionen Euro für 21 Stellen (13 hD; 7 gD; 1 mD). Davon entfallen rund

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

2,3 Millionen Euro auf Personalkosten und rund 0,7 Millionen Euro auf personalnahe Sachkosten. Der Bundespolizei entsteht über die Jahre 2027 bis 2031 ein aufwachsender jährlicher finanzieller Mehrbedarf in Höhe von rund 14,6 Millionen Euro für insgesamt 90 Planstellen (25 hD; 62 gD; 3 mD). Durch die gesetzliche Änderung entstehen einmalige investive Sachkosten in Höhe von 2,5 Millionen Euro sowie ab Anschaffung jährliche anfallende Kosten in Höhe von 2,3 Millionen Euro für Hardware, Lizenzen, Betrieb- und Wartung. Der mit der Aufgabenwahrnehmung verbundene Erfüllungsaufwand erfordert eine gesonderte haushälterische Vorsorge, da die herausragenden und strukturell verankerten Aufgaben im Rahmen einer reinen Priorisierung bestehender Tätigkeiten durch die Bundespolizei nicht angemessen umgesetzt werden können. Der Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für BSI, BKA und die BPOL soll im Einzelplan 06 ausgeglichen werden.

E. Erfüllungsaufwand

Das geplante Reglungsvorhaben dient im Wesentlichen der Abwehr erheblicher Gefahren im Bereich der IT-Sicherheit und ist daher von der „One in, one out“ Regel (sog. „Bürokratiebremse“) ausgenommen.

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Dem Normadressat Wirtschaft entsteht durch das geplante Regelungsvorhaben ein laufender Erfüllungsaufwand in Höhe von ca. 10 Millionen Euro und einmaliger Erfüllungsaufwand in Höhe von ca. 4,4 Millionen Euro.

Davon Bürokratiekosten aus Informationspflichten

Davon unterfallen 282.000 Euro auf Bürokratiekosten aus Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

Dem Normadressaten Verwaltung entsteht durch das geplante Regelungsvorhaben ein laufender Erfüllungsaufwand in Höhe von 35 Millionen Euro sowie ein einmaliger Erfüllungsaufwand in Höhe von 19,61 Millionen Euro auf Ebene des Bundes.

F. Weitere Kosten

Durch die im Gesetz für einzelne polizeiliche Befugnisse vorgesehenen richterlichen Anordnungen entstehenden den zuständigen Amtsgerichten Erfüllungsaufwände, beispielsweise für das BKA dem Amtsgericht Wiesbaden. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf die Verbraucherpreise, sind nicht zu erwarten.

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Beschlussempfehlung

Der Bundestag wolle beschließen,

a) den Gesetzentwurf auf Drucksachen 21/6585, 21/7406 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:

a) In Nummer 2 wird § 41a wie folgt geändert:

aa) Absatz 3 wird durch den folgenden Absatz 3 ersetzt:

„(3) Die besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Die besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3 dürfen nur durchgeführt werden, wenn die Abwehr der Gefahr durch eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 oder 2 nicht oder zumindest nicht gleichwertig möglich und auch im Übrigen die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre."

bb) Nach Absatz 5 Satz 2 wird der folgende Satz eingefügt:

„Bestehen insoweit begründete Zweifel, ist das informationstechnische System als privat zu betrachten."

b) Nummer 7 wird durch die folgende Nummer 7 ersetzt:

‚7. § 104 wird durch den folgenden § 104 ersetzt:

„§ 104

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer einer vollziehbaren Anordnung nach § 29 Absatz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach § 41a Absatz 1 Satz 1 Nummer 1 oder Absatz 9 Satz 1 zuwiderhandelt,
2. einer vollziehbaren Anordnung nach § 41a Absatz 11 Satz 1 zuwiderhandelt,
3. entgegen § 52 Absatz 1 Satz 2 in Verbindung mit einer Rechtsverordnung nach § 93 Absatz 1 dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt oder
4. einer vollziehbaren Anordnung nach § 96 Absatz 2 Satz 1 Nummer 4 zuwiderhandelt.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 mit einer Geldbuße bis zu fünfhunderttausend Euro, in den Fällen des Absatzes 2 Nummer 2 und 3 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 1 mit einer Geldbuße bis zu fünftausend

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Euro und in den Fällen des Absatzes 2 Nummer 4 mit einer Geldbuße bis zu tausend Euro geahndet werden.

(4) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist die in der Rechtsverordnung nach § 93 Absatz 1 bestimmte Bundespolizeibehörde. Sie teilt dem Luftfahrt-Bundesamt die Verhängung einer Geldbuße nach Absatz 2 Nummer 3 mit.“ ‘

2. Artikel 2 wird wie folgt geändert:

a) In Nummer 6 Buchstabe d wird in § 16 Absatz 7 Satz 1 jeweils die Angabe „Artikel 6“ durch die Angabe „Artikel 8“ ersetzt.

b) Nach Nummer 11 wird die folgende Nummer 12 eingefügt:

‚12. § 60 wird wie folgt geändert:

a) In Absatz 3 Satz 2 wird die Angabe „der die Einrichtung“ durch die Angabe „dem die Einrichtung“ ersetzt.

b) In Absatz 5 Satz 1 wird die Angabe „eine informationstechnisches System “ durch die Angabe „ein informationstechnisches System“ ersetzt.‘

c) Die bisherige Nummer 12 wird zu Nummer 13 und in der Angabe vor Buchstabe a wird die Angabe „§ 65“ durch die die Angabe „§ 68“ ersetzt.

d) Nach der neuen Nummer 13 wird die folgende Nummer 14 eingefügt:

‚14. Anlage 1 Spalte D wird wie folgt geändert:

a) In Nummer 1.1.1 wird die Angabe „Stromlieferanten nach § 3 Nummer 31c EnWG“ durch die Angabe „Stromlieferanten nach § 3 Nummer 94 EnWG“ ersetzt.

b) In Nummer 1.1.2 wird die Angabe „Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 3 EnWG“ durch die Angabe „Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 9 EnWG“ ersetzt.

c) In Nummer 1.1.3 wird die Angabe „Betreiber von Übertragungsnetzen nach § 3 Nummer 10 EnWG“ durch die Angabe „Betreiber von Übertragungsnetzen nach § 3 Nummer 16 EnWG“ ersetzt.

d) In Nummer 1.1.4 wird die Angabe „Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG“ durch die Angabe „Betreiber von Erzeugungsanlagen nach § 3 Nummer 43 EnWG“ ersetzt.

e) In Nummer 1.1.6 wird die Angabe „Aggregatoren nach § 3 Nummer 1a EnWG“ durch die Angabe „Digitale Energiedienste nach § 3 Nummer 26 EnWG“ ersetzt.

f) In Nummer 1.1.7 wird die Angabe „Betreiber von Energiespeicheranlagen nach § 3 Nummer 15d EnWG“ durch die Angabe „Betreiber von Energiespeicheranlagen nach § 3 Nummer 36 EnWG“ ersetzt.

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

g) In Nummer 1.1.8 wird die Angabe „Anbieter von Ausgleichsleistungen nach § 3 Nummer 1b EnWG“ durch die Angabe „Anbieter von Ausgleichsleistungen nach § 3 Nummer 3 EnWG“ ersetzt.‘

3. Artikel 3 wird wie folgt geändert:

a) Nummer 1 wird wie folgt geändert:

aa) Nach Buchstabe a wird der folgende Buchstabe b eingefügt:

‚b) Nach der Angabe zu § 53 wird die folgende Angabe eingefügt:

„§ 53a Informationstechnikbezogene Abwehrmaßnahmen“.‘

bb) Die bisherigen Buchstaben b bis d werden zu den Buchstaben c bis e.

cc) Nach Buchstabe e wird der folgende Buchstabe f eingefügt:

‚f) Nach der Angabe zu § 87 wird die folgende Angabe eingefügt:

„§ 87a Bußgeldvorschriften“.‘

b) In Nummer 3 wird § 3a Absatz 4 durch den folgenden Absatz 4 ersetzt:

„(4) Die Aufgaben und Befugnisse anderer Bundesbehörden bleiben unberührt. Das Bundeskriminalamt benachrichtigt die für die Polizeien zuständigen obersten Landesbehörden der betroffenen Länder und, soweit zuständig, andere Polizeibehörden des Bundes, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt. Die Aufgabenwahrnehmung erfolgt in gegenseitigem Benehmen.“

c) Nach Nummer 4 wird die folgende Nummer 5 eingefügt:

‚5. Nach § 53 wird der folgende § 53a eingefügt:

„§ 53a

Informationstechnikbezogene Abwehrmaßnahmen

Die §§ 68b bis 68f gelten für die Abwehr von Gefahren, die nicht zugleich Gefahren nach § 68a Absatz 2 sind, entsprechend.“ ‘

d) Die bisherigen Nummern 5 bis 8 werden zu den Nummern 6 bis 9.

e) Die bisherige Nummer 9 wird zu Nummer 10 und wird wie folgt geändert:

aa) § 68d Absatz 4 wird durch den folgenden Absatz 4 ersetzt:

„(4) Maßnahmen nach Absatz 1 dürfen nur durchgeführt werden, wenn die Abwehr der Gefahr durch eine Maßnahme nach § 68b oder § 68c nicht oder zumindest nicht gleichwertig möglich und auch im Übrigen die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie dürfen auch durchgeführt werden, wenn

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Dritte unvermeidbar betroffen werden. § 68c Absatz 2 Satz 2 und 3 gilt entsprechend.“

bb) § 68e Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Privat ist ein informationstechnisches System, wenn es als eigenes privat genutzt wird und aufgrund seiner technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten kann, dass bei einem Zugriff auf das System Umfang, Vielfalt und Qualität der Daten einen Einblick in wesentliche Teile der Lebensgestaltung der Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen. Bestehen insoweit begründete Zweifel, ist das informationstechnische System als privat zu betrachten.“

f) Die bisherige Nummer 10 wird zu Nummer 11.

g) Die bisherige Nummer 11 wird zu Nummer 12 und in Buchstabe a wird die Angabe „bis 53, 64 und 68d“ durch die Angabe „bis 53, 64 und 68d, auch in Verbindung mit § 53a,“ ersetzt.

h) Die bisherige Nummer 12 wird zu Nummer 13.

i) Die bisherige Nummer 13 wird zu Nummer 14 und in Buchstabe a wird die Angabe „53, 64 und 68d in Verbindung mit 68e“ durch die Angabe „53, 64 und 68d in Verbindung mit 68e, auch in Verbindung mit § 53a,“ ersetzt.

j) Die bisherige Nummer 14 wird durch die folgende Nummer 15 ersetzt:

‚15. Nach § 87 wird der folgende § 87a eingefügt:

„§ 87a

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach § 60a Absatz 2 oder § 68f Absatz 1 zuwiderhandelt oder
2. einer vollziehbaren Anordnung nach § 68b oder § 68c Absatz 2 Satz 1, jeweils auch in Verbindung mit § 53a, zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 mit einer Geldbuße bis zu fünfzigtausend Euro und in den Fällen des Absatzes 1 Nummer 2 mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundeskriminalamt.“ ‘

k) Nach Nummer 15 wird die folgende Nummer 16 eingefügt:

‚16. § 90 wird wie folgt geändert:

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

a) In Absatz 1 wird die Angabe „Abschnitt 5“ durch die Angabe „den Abschnitten 5 und 8a“ ersetzt.

b) In Absatz 3 Satz 1 wird die Angabe „51 und 64“ durch die Angabe „51, 64 und 68d, auch in Verbindung mit 53c,“ ersetzt.‘

4. In Artikel 6 wird die Angabe „Artikel 3 Nummer 6, 7 und 9 (§§ 60, 60a und 68a bis 68e des Bundeskriminalamtgesetzes“ durch die Angabe „Artikel 3 Nummer 5, 7, 8 und 10 (§§ 53a, 60, 60a und 68a bis 68e des Bundeskriminalamtgesetzes“ ersetzt.

5. Nach Artikel 6 wird der folgende Artikel 7 eingefügt:

„Artikel 7

Evaluierung

(1) Das Bundesministerium des Innern evaluiert die Wirksamkeit und die Auswirkungen der durch dieses Gesetz eingeführten oder geänderten Regelungen spätestens bis zum 1. Januar 2029.

(2) Das Bundesministerium des Innern legt dem Deutschen Bundestag spätestens sechs Monate nach Abschluss der Evaluierung einen Bericht über dessen Ergebnisse vor.“

6. Der bisherige Artikel 7 wird zu Artikel 8.;

b) folgende Entschließung anzunehmen:

I. Der Deutsche Bundestag stellt fest:

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland als führende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller Cyberangriffe mit großem Wirkpotential. Angesichts der geopolitischen Lage gewinnen auch hybride Bedrohungen zunehmend an Bedeutung. Der Krieg in der Ukraine verdeutlicht, wie essenziell Cybersicherheit für einen modernen Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sicheren Nutzung der Informationstechnologie und der zugrundeliegenden Kommunikationsinfrastruktur ist elementare Voraussetzung für das Funktionieren des Gemeinwesens.

Mit dem Gesetz zur Stärkung der Cybersicherheit werden wirksame, angemessene und rechtsklare gesetzliche Grundlagen geschaffen, um derartige Cyberangriffe erkennen und abwehren zu können. So werden die Befugnisse des BSI zur Aufklärung und Detektion konkreter Angriffe und langfristig laufender Angriffskampagnen sowie zur Detektion konkreter Vorbereitungshandlungen ausgebaut. Insbesondere gegen groß angelegte Cyberangriffe mit großem Schadenspotential bieten präventive Maßnahmen in den eigenen IT-Systemen allein allerdings keinen hinreichenden Schutz. Für die Polizeien des Bundes werden daher auch Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen, um gravierende Folgeschäden abwenden oder minimieren zu können. Dazu zählen neben der Detektion von Angriffsmustern und -strukturen auch Maßnahmen im Netz, die den Schaden begrenzen, und - als letztes Mittel - der Eingriff in Systeme der Angreifer. Damit werden die Fähigkeiten zur aktiven Cyberabwehr gezielt ausgebaut.

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Mit der Ausweitung staatlicher Cyberfähigkeiten und -befugnisse übernehmen dann neben der Bundeswehr mehrere Bundesbehörden eigenständige Aufgaben im Bereich der aktiven Cyberabwehr. Cyberabwehrmaßnahmen sind an strenge Voraussetzungen geknüpft und bergen auch Risiken. Ein Datenstrom kann nur einmal umgeleitet oder eine Domain nur einmal beschlagnahmt werden. Dazu zählt auch das operative Risiko, dass eine Maßnahme einer Behörde unwissentlich laufende Maßnahmen einer anderen Behörde oder von Dienststellen im Geschäftsbereich des BMVg gefährden oder dem Gegner offenbaren kann, besonders bei langfristig angelegten Maßnahmen. Daher ist bei der operativen Fallbearbeitung ein behördenübergreifendes enges Zusammenwirken von BSI, Polizeien, Nachrichtendiensten und der Bundeswehr und ein gemeinsames unverstelltes Lagebild unverzichtbar und es braucht einen abgestimmten Rahmen zum Umgang mit potenziellen Konflikten zwischen den Sicherheitsbehörden.

Entscheidend für ein Mehr an Cybersicherheit ist daher neben den notwendigen neuen Befugnissen ein einheitliches und ganzheitliches Lagebild und ein Gesamtüberblick über alle Cyberabwehrmaßnahmen sowie ein enges Zusammenwirken aller an der Cyberabwehr beteiligten Akteure. Ein wesentlicher Ort dafür ist die zentrale Cybersicherheitsbehörde des Bundes, das BSI, und das dort verortete Nationale Cyberabwehrzentrum (Cyber-AZ). Das Cyber-AZ wurde im Zuge der Umsetzung der Cybersicherheitsstrategie Deutschland 2011 als gemeinsame, behörden- und institutionenübergreifende Plattform für einen verbesserten und beschleunigten Informationsaustausch zwischen den beteiligten Behörden und Einrichtungen und zur stärkeren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle in Deutschland eingerichtet. Es bietet eine verlässliche und praxiserprobte Plattform zur Koordinierung herausgehobener Cybervorfälle, auf die für die Koordinierung der Cyberabwehr aufgesetzt werden kann.

Die aktuelle Cybersicherheitsstrategie für Deutschland der Bundesregierung aus dem Jahr 2021 bildet den Rahmen bis 2026. Notwendig ist daher eine Weiterentwicklung der Cybersicherheitsstrategie der Bundesregierung mit dem Ziel einer klaren Rollen- und Aufgabenverteilung und einem intensiveren Informationsaustausch. Zudem ist das BSI weiter zu stärken und zu einer zentralen Stelle für Fragen der Informations- und Cybersicherheit auszubauen.

II. Der Deutsche Bundestag fordert die Bundesregierung der 21. Wahlperiode auf:

1. Die anstehende Weiterentwicklung der Cybersicherheitsstrategie 2026 vorzulegen und dabei angesichts der aktuellen geopolitische Bedrohungslage durch Cyberangriffe insbesondere auch den Rahmen für das Cyber-Abwehrzentrum (AZ) als zentrale und behördenübergreifende Plattform für die Cyberabwehr weiterzuentwickeln;

2. Das mit der Cybersicherheitsstrategie 2011 eingerichtete Nationale Cyber-AZ weiter als maßgeblichen Akteur bei Cyberangriffen auszubauen und den Informationsaustausch aller an der IT-Sicherheit beteiligter Akteure, insbesondere auch mit Blick auf aktive Cyberabwehrmaßnahmen, auf dieser Plattform zu intensivieren;

3. Das Cyber-AZ als zentrale Koordinationsplattform auszugestalten, auf der die behördenübergreifende Erst-Abstimmung von Cybervorfällen stattfindet. Hier wird zuerst festgestellt, ob ein Vorfall einen staatlichen Hintergrund

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

haben könnte oder nicht. Bei der operativen Fallbearbeitung ist ein behördenübergreifendes Zusammenwirken von BSI, Polizeien, Nachrichtendiensten und der Bundeswehr unverzichtbar. Die Behörden sollen sich, unter Wahrung der notwendigen Geheimhaltung, über das Ergreifen von Maßnahmen gegenseitig informieren. Das Cyber-AZ ist der zentrale Ort für die Abklärung etwaiger operativer Betroffenheiten anderer Sicherheitsbehörden.

4. Eine stärkere und schnellere Einbindung der Wirtschaft und der Länder für die Erstellung ganzheitlicher und sektoraler Lagebilder sicherzustellen. Die IMK hat 2024 das Konzept und die Voraussetzungen (u.a. zur sicheren technischen Anbindung) für die Einbindung der Länder in das Cyber-AZ beschlossen. Die Umsetzung soll priorisiert werden;

5. Das BSI im Rahmen der Weiterentwicklung der Cybersicherheitsstrategie als die zentrale Cybersicherheitsbehörde des Bundes weiter zu stärken. Das Cyber-AZ soll auch zukünftig im BSI verortet sein. Entscheidend für die Cybersicherheit ist – unter der Wahrung der notwendigen Geheimhaltung – ein einheitliches, ganzheitliches und unverstelltes IT-Lagebild – inklusive der aktuellen aktiven Cyberabwehrmaßnahmen. Die Weiterentwicklung des Cyber-AZ in der anstehenden Cybersicherheitsstrategie soll ein solches gemeinsames ganzheitliches Lagebild sicherstellen. Im Bereich der aktiven Cyberabwehr soll eine klare Rollen- und Aufgabenverteilung sichergestellt werden;

6. Mit Blick auf den ressourceneffizienten Einsatz und insbesondere mit Blick auf die digitale Souveränität und den Abbau bestehender problematischer Abhängigkeiten die notwendigen Technischen Mittel für eine wirksame Abwehr von Cyberangriffen zu entwickeln.;

c) den Antrag auf Drucksache 21/6653 abzulehnen.

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Berlin, den 11. November 2026

Der Innenausschuss

Josef Oster
Amtierender Vorsitzender

Marc Henrichmann
Berichterstatter

Steffen Janich
Berichterstatter

Daniel Baldy
Berichterstatter

Dr. Konstantin von Notz
Berichterstatter

Jan Krampe
Berichterstatter

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Bericht der Abgeordneten Marc Henrichmann, Steffen Janich, Daniel Baldy, Dr. Konstantin von Notz und Jan Krampe

I. Überweisung

Zu Buchstabe a

Der Gesetzentwurf auf **Drucksachen 21/6585** wurde in der 86. Sitzung des Deutschen Bundestages am 25. Juni 2025 an den Innenausschuss federführend sowie an den Ausschuss für Recht und Verbraucherschutz, den Haushaltsausschuss, den Ausschuss für Wirtschaft und Energie, den Verteidigungsausschuss, den Verkehrsausschuss und den Ausschuss für Digitales und Staatsmodernisierung zur Mitberatung überwiesen. Dem Haushaltsausschuss wurde der Gesetzentwurf zudem gemäß § 96 der Geschäftsordnung überwiesen. Die Unterrichtung durch die Bundesregierung zur Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung lag auf **Drucksache 21/7406** vor. Der Parlamentarische Beirat für nachhaltige Entwicklung und Zukunftsfragen beteiligte sich gutachtlich (Ausschussdrucksache 21(26)67-8).

Zu Buchstabe b

Der Antrag auf **Drucksache 21/6653** wurde in der 86. Sitzung des Deutschen Bundestages am 25. Juni 2026 an den Innenausschuss federführend sowie an den Ausschuss für Recht und Verbraucherschutz und den Ausschuss für Digitales und Staatsmodernisierung zur Mitberatung überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Zu Buchstabe a

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 59. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen.

Der **Ausschuss für Wirtschaft und Energie** hat in seiner 59. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen.

Der **Haushaltsausschuss** hat in seiner 59. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen. Seinen Bericht nach § 96 der Geschäftsordnung wird er gesondert abgeben.

Der **Verteidigungsausschuss** hat in seiner 41. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen.

Der **Verkehrsausschuss** hat in seiner 42. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen.

Der **Ausschuss für Digitales und Staatsmodernisierung** hat in seiner 38. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke die Annahme des Gesetzentwurfs auf Drucksachen 21/6585, 21/7406 in geänderter Fassung empfohlen.

Zu Buchstabe b

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 59. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion Die Linke bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN sowie von zwei Mitgliedern der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 21/6653 empfohlen.

Der **Ausschuss für Digitales und Staatsmodernisierung** hat in seiner 38. Sitzung am 11. November 2026 mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion Die Linke bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN die Ablehnung des Antrags auf Drucksache 21/6653 empfohlen.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Zu Buchstabe a

Der Innenausschuss hat in seiner 38. Sitzung am 8. Juli 2026 zu Drucksachen 21/6585, 21/7406 einstimmig beschlossen, eine öffentliche Anhörung durchzuführen. Die öffentliche Anhörung, an der sich sieben von den Fraktionen benannte Sachverständige beteiligt haben, hat der Innenausschuss in seiner 43. Sitzung am 5. Oktober 2026 durchgeführt. Hinsichtlich des Ergebnisses der Anhörung wird auf das Protokoll der 43. Sitzung (Protokoll 21/43) verwiesen.

Der **Innenausschuss** hat den Gesetzentwurf auf Drucksachen 21/6585, 21/7406 in seiner 49. Sitzung am 11. November 2026 abschließend beraten und empfiehlt die Annahme des Gesetzentwurfs in der aus der Beschlussempfehlung ersichtlichen Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, BÜNDNIS 90/DIE GRÜNEN und Die Linke.

Die Änderungen entsprechen dem Änderungsantrag der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)251, der zuvor mit den Stimmen der Fraktionen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD und Die Linke bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN angenommen wurde.

Zudem hat der Innenausschuss die Entschließung der Fraktionen der CDU/CSU und SPD mit dem aus der Beschlussempfehlung ersichtlichen Wortlaut auf Ausschussdrucksache 21(4)252 mit den Stimmen der Fraktionen CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktionen AfD und Die Linke angenommen.

Zu Buchstabe b

Der **Innenausschuss** hat den Antrag auf Drucksache 21/6653 in seiner 49. Sitzung am 11. November 2026 abschließend beraten und empfiehlt die Ablehnung des Antrags mit den Stimmen der Fraktionen der CDU/CSU, AfD und SPD gegen die Stimmen der Fraktion Die Linke bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN.

IV. Begründung

1. Begründung zum Änderungsantrag

Zur Begründung allgemein wird auf Drucksache 21/6585 verwiesen. Die vom Innenausschuss auf Grundlage des Änderungsantrags der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 21(4)251 vorgenommenen Änderungen begründen sich wie folgt:

Zu Nummer 1 (Artikel 1)

Zu Buchstabe a

Zu § 41a Absatz 3

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Im Rahmen der Auswahl des Mittels der Gefahrenabwehr ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dies ergibt sich bereits aus § 16 BPolG. Die Neufassung von § 41a Absatz 3 dient der Klarstellung, dass Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 3 in der Regel als eingriffsintensiver als Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 1 oder 2 bewertet werden. Ergibt sich aus den Umständen des Einzelfalls nichts anderes, sind die Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 1 oder 2 daher vorranging einzusetzen, wobei bei der Auswahl des konkreten Mittels wiederum der Grundsatz der Verhältnismäßigkeit zu beachten ist.

Bevor eine Maßnahmen nach § 41a Absatz 1 Satz 1 durchgeführt wird, ist der Sachverhalt soweit aufzuklären, dass festgestellt werden kann, dass die vorgenommene Maßnahme verhältnismäßig ist.

Zu § 41a Absatz 5 Satz 3

Der neu eingefügte § 41a Absatz 5 Satz 3 regelt eine Zweifelsregelung zugunsten privater informationstechnischer Systeme. Liegen begründete Zweifel hinsichtlich der Natur und Nutzung des Systems vor (privat oder nicht-privat), ist, um der besonderen Eingriffsintensität der Maßnahme nach § 41a Absatz 1 Satz 1 Nummer 3 Rechnung zu tragen, von einem privaten System im Sinne des § 41a Absatz 5 Satz 2 auszugehen. Dies hat zur Folge, dass ein informationstechnisches System nur dann als nicht-privates behandelt werden darf, wenn es mit der entsprechenden Sicherheit als solches identifiziert werden kann.

Zu Buchstabe b

Die Neufassung des Änderungsbefehls Nummer 7 ist eine Folgeänderung aufgrund der Anpassung des Gesetzes zur Modernisierung des Bundespolizeigesetzes entsprechend der Beschlussempfehlung des Innenausschusses des Deutschen Bundestages (BT-Drs. 21/6990). Entsprechend der Beschlussempfehlung des Innenausschusses wurde der Verstoß gegen die Meldeauflage in § 104 Absatz 1 BPolG bußgeldbewehrt. Dadurch musste der § 104 angepasst werden.

Zu Nummer 2 (Artikel 2)

Zu Buchstabe a

Korrektur des Datierungsbefehls.

Zu Buchstabe b

Korrektur eines Tippfehlers.

Zu Buchstabe c

Es handelt sich um notwendigen Korrekturbedarf, der sich aus der Verschiebung des § 65 BSIG in den § 68 BSIG durch das CRA-Durchführungsgesetz ergibt (Gesetz zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) BT-Drs. 21/6134 und 21/8622).

Zu Buchstabe d

Korrektur von Verweisfehlern.

Die Änderung von Nummer 1.1.6 ist zudem eine Folgeänderung aus dem NIS2-Umsetzungsgesetz. Mit dem NIS2-Umsetzungsgesetz sollten auch digitale Energiedienste unter die Regulierung des IT-Sicherheitskataloges genommen werden. § 5c Absatz 1 Nummer 3 EnWG erfasst Betreiber digitaler Energiedienste, die besonders wichtige oder wichtige Einrichtungen nach § 28 sind. Die aktuelle Verweiskette in EnWG und BSIG führt dazu, dass nur Aggregatoren als Teilausschnitt digitaler Energiedienste effektiv reguliert werden.

Zu Nummer 3 (Artikel 3)

Zu Buchstabe a

Änderung der Inhaltsübersicht als Folgeänderung zur Ergänzung der neuen §§ 53a und 87a (s. zu den Buchstaben c und j).

Zu Buchstabe b

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Die in die neue Aufgabe nach § 3a BKAG nun eingefügte Benehmensregelung orientiert sich an der Regelung in § 5 Absatz 2 Satz 2 BKAG und sieht vor, dass sich das BKA bei Wahrnehmung dieser Aufgabe mit anderen zuständigen Polizeibehörden des Bundes und der Länder ins Benehmen setzt.

Zu Buchstabe c

Der bisherige Gesetzentwurf sah die Anwendung cyberspezifischer Befugnisse nur zur Abwehr von Angriffen auf die IT-Sicherheit vor. Denn nach der bisherigen Systematik kamen die neuen Befugnisse nach den §§ 68b bis 68d BKAG auch für die bestehenden Aufgaben nach § 5 BKAG (Gefahren des internationalen Terrorismus) oder den §§ 6, 7 oder 8 BKAG nur für Fallkonstellationen in Betracht, in denen parallel eine Gefahr für die IT-Sicherheit im Sinne von § 3a Absatz 2 BKAG verwirklicht wird.

Es zeigt sich jedoch zunehmend, dass es auch Fallkonstellationen gibt, in denen durch die Angreiferseite IT-Systeme zur Herbeiführung einer realweltlichen Gefahr genutzt werden, dabei aber gerade keine Gefahr für die IT-Sicherheit selbst realisiert wird.

Ein Beispiel dafür sind unkonventionelle Spreng- und Brandvorrichtungen (USBV), die über eine Internetverbindung gesteuert werden.

In bestimmten Fällen kann eine Abwehr solcher Gefahren ausschließlich durch cyberspezifische Befugnisse erfolgen, z. B. wenn die zur Tatausübung genutzte Informationstechnik bekannt ist, die Angreifer aber nicht lokalisierbar sind oder die Tatmittel selbst nicht schnell genug unschädlich gemacht werden können.

Die Neuregelung erlaubt es dem BKA daher, die neuen informationstechnikbezogenen Abwehrmaßnahmen nach den §§ 68b bis 68d im Rahmen der Aufgabe nach § 5 auch dann einzusetzen, wenn nicht gleichzeitig eine Gefahr im Sinne des § 3a Absatz 2 vorliegt. Dazu gehört u.a. das Umleiten von Datenverkehr nach § 68c zwischen USBV und Steuerungsgerät zur Unterbrechung der Verbindung zwischen den Geräten oder das Auslesen, Löschen oder Verändern von gefahrgegenständlichen Daten nach § 68d, z. B. das Löschen von Daten, über die eine USBV gesteuert oder ausgelöst werden soll, um die Steuerung zu übernehmen oder eine Auslösung der USBV zu verhindern. Für die Befugnisse nach den §§ 68b bis 68d gelten auch in Fällen des § 53a die besonderen Bestimmungen und Verfahrensvorschriften wie z. B. § 68e, 68f, 74 oder 79.

Zu Buchstabe d

Folgeänderung.

Zu Buchstabe e Doppelbuchstabe aa

Die Ergänzung dient der Klarstellung, dass der Grundsatz der Verhältnismäßigkeit bei Maßnahmen nach § 68d zu beachten ist sowie dass die Befugnisse nach § 68d in der Regel als eingriffsintensiver gegenüber den Maßnahmen nach § 68b und § 68c eingeordnet werden. Ergibt sich aus den Umständen des Einzelfalls nichts anderes, sind die Maßnahmen nach den §§ 68b und 68c daher vorranging einzusetzen, wobei auch dabei der Grundsatz der Verhältnismäßigkeit zu beachten ist.

Bevor die Maßnahmen nach §§ 68b bis 68d durchgeführt werden, ist der Sachverhalt soweit aufzuklären, dass festgestellt werden kann, dass die vorgenommene Maßnahme verhältnismäßig ist.

Zu Buchstabe e Doppelbuchstabe bb

Die Ergänzung enthält eine Zweifelsregelung zugunsten privater informationstechnischer Systeme. Liegen begründete Zweifel hinsichtlich der Natur oder Nutzung des Systems vor (privat oder nicht-privat), ist, um der besonderen Eingriffsintensität der Maßnahme nach § 68d Rechnung zu tragen, von einem privaten System im Sinne des § 68e Absatz 2 auszugehen. Dies hat zur Folge, dass ein informationstechnisches System nur dann als nicht-privates behandelt werden darf, wenn es mit der entsprechenden Sicherheit als solches identifiziert werden kann.

Zu den Buchstaben f bis i

Folgeänderungen.

Zu Buchstabe j

Folgeänderung sowie Änderung der Bußgeldvorschrift. Der bisherige Gesetzentwurf basierte auf der Annahme, dass vor Inkrafttreten dieses Gesetzes ein § 87a (vgl. BT-Drucksache 21/6131 „Entwurf eines Gesetzes zur Stär-

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

kung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“) geschaffen wird. Da das Inkrafttreten des genannten Entwurfs zeitlich nach diesem Gesetz zu erwarten ist, erfolgt die Einführung eines Bußgeldparagrafen nun in diesem Gesetz.

Zu Buchstabe k

Die Änderung dient der Korrektur und bezieht den neuen Abschnitt 8a in die Regelungen des § 90 zur gerichtlichen Zuständigkeit ein. Daraus ergibt sich u. a. die Zuständigkeit des Amtsgerichts am Sitz des Bundeskriminalamts für gerichtliche Entscheidungen nach § 68e.

Zu Nummer 4 (Artikel 6)

Mit der Änderung wird mit Blick auf den neuen § 53a BKAG dem Zitiergebot des Artikels 19 Absatz 1 Satz 2 des Grundgesetzes nachgekommen.

Zu Nummer 5 (Artikel 7 – Evaluierung)

Mit der Einfügung des neuen Artikels 7 wird eine Verpflichtung zur Evaluierung der durch das Gesetz eingeführten oder geänderten Regelungen geschaffen.

Die Evaluierung dient der Überprüfung, inwieweit die mit dem Gesetz verfolgten Ziele zur Stärkung der Cybersicherheit tatsächlich erreicht werden und ob die hierfür vorgesehenen Maßnahmen wirksam sind.

Im Rahmen der Evaluierung ist zu untersuchen, inwieweit die gesetzlichen Regelungen zur Gefahrenabwehr und zur Verbesserung der Cybersicherheit beigetragen haben. Die Evaluierung soll insbesondere Erkenntnisse über die Praktikabilität der gesetzlichen Regelungen und die Zusammenarbeit der zuständigen Behörden liefern.

Dabei sind insbesondere zu berücksichtigen:

1. die Wirksamkeit der durchgeführten Maßnahmen zur Erkennung und Abwehr von Cyberangriffen sowie zur Eindämmung der Ausbreitung schädlicher informationstechnischer Infrastrukturen,
2. die Auswirkung der durchgeführten Maßnahmen auf die Sicherheit und Funktionsfähigkeit der betroffenen informationstechnischen Systeme sowie die Auswirkung auf die Betroffenheit der Grundrechte von am Angriff nicht beteiligten Dritten und deren Gewichtung im Rahmen der Verhältnismäßigkeit,
3. die Häufigkeit und die Ergebnisse der Anwendung der neu geschaffenen Befugnisse sowie
4. die Praktikabilität der gesetzlichen Regelungen und die Zusammenarbeit der zuständigen Behörden.

Die Evaluierung erfolgt unter Berücksichtigung geeigneter qualitativer Kriterien. Hierzu sind insbesondere die Erfahrungen der für den Vollzug zuständigen Behörden und der von den Regelungen betroffenen zuständigen Stellen einzubeziehen. Die Evaluierung soll unter Beteiligung wissenschaftlichen Sachverstandes erfolgen.

Die Unterrichtung des Deutschen Bundestages, dort des zuständigen Innenausschusses und des Ausschusses für Digitales und Staatsmodernisierung, gewährleistet, dass die Ergebnisse der Evaluierung für die parlamentarische Befassung und die Prüfung eines etwaigen gesetzgeberischen Anpassungsbedarfes zur Verfügung stehen.

Zu Nummer 6 (Artikel 8)

Es handelt sich um eine redaktionelle Folgeänderung aufgrund der Einfügung des neuen Artikels 7.

2. Begründung der Fraktionen im Ausschuss

Die **Fraktion der CDU/CSU** betont die Zunahme der Cyberbedrohungen sowie der durch entsprechende Angriffe verursachten Schäden. Das BKA und die Bundespolizei sollten künftig in die Lage versetzt werden, den Betrieb eines informationstechnischen Systems einschränken und gegebenenfalls unterbinden zu können. Konkret ermöglicht werden solle die Umleitung von schädlichen Datenverkehren sowie das Auslesen, Löschen und Verändern von gefahrgegenständlichen Daten in IT-Systemen. Entsprechende Maßnahmen seien ausschließlich zur Gefahrenabwehr, nicht zum Zweck der Strafverfolgung zulässig. Das BSI sei bereits in der Vergangenheit durch zusätzliche Aufgaben und Befugnisse gestärkt worden. Nunmehr solle es insbesondere zur frühzeitigen Erkennung von Cyberbedrohungen („Threat Hunting“), auch im Bereich der Kommunikationstechnik der Bundeswehr, befugt werden. Dies umfasse auch das sogenannte „Pre-Positioning“, bei dem Angreifer bereits Zugang zu einem

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

IT-System erlangt hätten, der Angriff jedoch noch nicht durchgeführt worden sei. Das BSI solle bereits vor der eigentlichen Tatbegehung und dem Eintritt eines Schadens tätig werden können. Weitere Regelungen beträfen Anordnungsbefugnisse gegenüber digitalen Diensteanbietern, den Umgang mit gefährlichen Domainnamen sowie die Automatisierung von Schutzmaßnahmen, insbesondere für Betreiber kritischer Infrastrukturen. Gemeinsam mit den bereits eingeführten Systemen zur Angriffserkennung bildeten diese Maßnahmen die Grundlage für das Projekt „Cyberdome", das Sensorik, Analyse und Abwehr miteinander verknüpfe. Mit dem KRITIS-Dachgesetz und der NIS2-Umsetzung seien bereits passive Schutzmaßnahmen und Systeme zur Angriffserkennung gestärkt worden. Der Cyber Resilience Act verankere zudem den Grundsatz „Security by Design“, wonach Cybersicherheit bereits im Entwicklungs- und Produktionsprozess berücksichtigt werde. Der vorliegende Gesetzentwurf ergänze diese Maßnahmen um die aktive Cyberabwehr. Die vorgesehenen Befugnisse würden von den zuständigen Praktikern ausdrücklich benötigt und ermöglichten es, künftig auf Cyberangriffe aktiv zu reagieren. Sie wirbt ausdrücklich um Zustimmung zum Gesetzentwurf.

Die **Fraktion der AfD** sieht die Cybersicherheit als ein zentrales Thema des 21. Jahrhunderts an. Der Microsoft Digital Defense Report 2026 weise Deutschland als das weltweit am vierthäufigsten betroffene Zielland von Cyberangriffen aus, innerhalb der EU sei Deutschland das am häufigsten von Cyberangriffen betroffene Land. Sie befürwortet grundsätzlich, dass der Staat für den Schutz gegen die neuen Bedrohungen effiziente Mittel erhalte. Allerdings könne sie die geplanten Maßnahmen in der Gesamtheit nicht mittragen. Die Nutzungsuntersagung eines IT-Systems gegenüber deutschen Unternehmen sollte gesetzlich befristet werden. Es helfe den Unternehmen nicht, wenn sie zwar vor einem Cyberangriff geschützt würden, allerdings von Insolvenz bedroht seien, weil der Staat ihnen den Fortbetrieb ihres Geschäfts untersage. Darüber hinaus differenziere die neue Befugnis der Bundespolizei zum Löschen, Auslesen und Verändern von Daten nicht danach, ob der Betreiber der geschädigten IT-Systeme oder Dritte gut- oder bösgläubig seien. Die Einführung eines Richtervorbehalts für das Auslesen, Löschen und Verändern von relevanten Daten erachte sie als nachvollziehbar. Es bestünden jedoch erhebliche Zweifel, ob die Amtsgerichte kurzfristig in der Lage seien, die Tragweite entsprechender Entscheidungen angemessen zu beurteilen. Hierfür seien gesonderte Schulungen für Richterinnen und Richter notwendig. Die ursprünglich vom Bundesinnenminister vorgesehenen Maßnahmen zur aktiven Cyberabwehr („Hackbacks“) gegen Netzwerke und Server im außereuropäischen Ausland seien nicht mehr enthalten. Diese seien jedoch nach den Erfahrungen des BSI erforderlich, um gezielten Cyberangriffen wirksam begegnen zu können. Positiv sei der durch den Änderungsantrag verbesserte Schutz privater IT-Systeme zu bewerten. Die bestehenden Mängel würden durch den Änderungsantrag jedoch nicht behoben. Sie könne dem Gesetzentwurf daher insgesamt nicht zustimmen.

Die **Fraktion der SPD** betont, dass für sämtliche polizeilichen Maßnahmen der Grundsatz der Verhältnismäßigkeit gelte. Dies werde durch den Gesetzesentwurf für Maßnahmen der Bundespolizei und des BKA nochmals ausdrücklich konkretisiert. Diese seien nur so lange zulässig, wie die jeweilige Gefahrenlage fortbestehe und der Eingriff weiterhin verhältnismäßig sei. Zudem würden die Regelungen zu Eingriffen in private IT-Systeme präzisiert und gegenseitige Informationspflichten der Polizeibehörden vorgesehen, um Überschneidungen bei der Durchführung von Maßnahmen zu vermeiden. Hiermit würden insbesondere Erkenntnisse aus der Sachverständigenanhörung aufgegriffen. Auch das Cyberabwehrzentrum leiste bereits einen wichtigen Beitrag zum behördenübergreifenden Informationsaustausch zwischen den Polizeibehörden, den Nachrichtendiensten, der Bundeswehr und den Ländern. Seine Funktion sowie die Zusammenarbeit der beteiligten Behörden sollten durch den Gesetzentwurf und die Entschließung weiter gestärkt werden.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** teilt die Einschätzung der erheblichen Bedrohung Deutschlands durch Cyberangriffe sowie die Notwendigkeit einer gesetzlichen Regelung zur Stärkung der Cyberabwehr. Allerdings müsse der Schwerpunkt zunächst auf defensiven Maßnahmen liegen. Das Schutzniveau ließe sich bereits durch einfache Maßnahmen und verbindliche Sicherheitsstandards für Unternehmen und Behörden sowie gezielte Investitionsanreize erheblich verbessern. Entsprechende Maßnahmen bleibe die Bundesregierung weiter schuldig. Zudem blieben im Rahmen der vorgesehenen Regelungen wesentliche Zuständigkeitsfragen der Sicherheitsbehörden ungeklärt. Sie kritisiert darüber hinaus das Fehlen eines gesetzlich geregelten Schwachstellenmanagements. Bei der Nutzung von IT-Sicherheitslücken für offensive Cyberabwehrmaßnahmen müsse abgewogen werden, welche Schwachstellen genutzt und welche zum Schutz staatlicher Systeme geschlossen werden müssten. Beispielhaft nennt sie den Cyberangriff auf das Berliner Landesnetz. Insgesamt könne sie dem Gesetzesentwurf daher trotz des dringenden Handlungsbedarfs nicht zustimmen.

Die **Fraktion Die Linke** bekräftigt das Erfordernis, auf Bedrohungen aus dem Cyberraum auch mit Eingriffen in informationstechnische Systeme zu reagieren, um beispielsweise gegen Botnetze vorzugehen. Sie kritisiert zu-

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

gleich, dass der Gesetzentwurf entsprechende Befugnisse für verschiedene Behörden vorsehe. Dies gelte insbesondere für die Bundespolizei, hier seien Angriffe auf die IT-Infrastruktur des europäischen Migrationsdatenmanagements höchst unwahrscheinlich, aber denkbar. Der Gesetzentwurf lasse offen, ob die EU, das Bundesverwaltungsamt als technischer Betreiber, das BSI oder die Bundespolizei für die Abwehr entsprechender Cyberangriffe zuständig seien. Gleiches gelte für Bahnanlagen, für deren Schutz als kritische Infrastruktur ebenfalls das BSI zuständig sei. Auch die pauschale Aufgabenzuweisung im Bundeskriminalamtgesetz sei nicht überzeugend. Zudem solle das BKA im Wege der Amtshilfe für die Landeskriminalämter tätig werden können, sofern deren Rechtsgrundlagen entsprechende Maßnahmen vorsähen. Dies führe zu einer schleichenden Verlagerung der Gefahrenabwehr auf den Bund, ohne eine klare und grundsätzliche Zuständigkeitsregelung zu schaffen. Dies sei mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbar. Gleiches gelte für die vorgesehenen Hackback-Befugnisse, da der Zielkonflikt zwischen staatlichen Eingriffen in IT-Systeme und deren Schutz nicht hinreichend geregelt werde. Insbesondere fehle weiterhin das von der Mehrheit der Sachverständigen geforderte Schwachstellenmanagement. Die vorgesehenen Übermittlungspflichten des BSI gegenüber den Sicherheitsbehörden verschärften diese Problematik und schwächten zugleich die Stellung des BSI. Die Befugnisse des BSI seien grundsätzlich vertretbar, die vorgesehene personelle Ausstattung jedoch deutlich zu gering.

Berlin, den 11. November 2026

Marc Henrichmann
Berichterstatter

Steffen Janich
Berichterstatter

Daniel Baldy
Berichterstatter

Dr. Konstantin von Notz
Berichterstatter

Jan Krampe
Berichterstatter

Vorabfassung – wird durch die lektorierte Fassung ersetzt.