



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

Schriftliche Stellungnahme

von Prof. Dr. Dennis-Kenji Kipker, Cyberintelligence Institute,
Frankfurt am Main vom 1. Oktober 2026

zu dem

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

Deutscher Bundestag
Ausschuss für Inneres
Platz der Republik 1
11011 Berlin

cyberintelligence.institute
MesseTurm // Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

Prof. Dr. Dennis-Kenji Kipker
Research Director & Founder
Dennis.Kipker@cyberintelligence.institute

Per E-Mail: innenausschuss@bundestag.de

Berlin, 1. Oktober 2026

Betreff: **Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit, BT-Drucksache 21/6585**

Berufener Sachverständiger:

Prof. Dr. Dennis-Kenji Kipker, Forschungsdirektor und Gründer cyberintelligence.institute

Sehr geehrter Herr Oster,
sehr geehrte Mitglieder des Ausschusses,
sehr geehrte Damen und Herren,

ich bedanke mich für die Möglichkeit zur fachlichen Stellungnahme des benannten Gesetzes im Rahmen der nachfolgenden Ausführungen:

Der Entwurf eines Gesetzes zur Stärkung der Cybersicherheit reagiert auf die zunehmende Zahl und technische Komplexität von Cyberangriffen und soll die staatlichen Möglichkeiten zu ihrer Abwehr deutlich erweitern.¹ Hierzu werden insbesondere neue operative Befugnisse für das Bundeskriminalamt (BKA) und die Bundespolizei geschaffen, die bis zur Untersagung des Betriebs informationstechnischer Systeme, zur Umleitung und Aufzeichnung von Datenverkehr sowie zum Auslesen, Löschen und Verändern von Daten in informationstechnischen Systemen reichen. Zugleich werden Aufgaben und Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erweitert, insbesondere bei der Umleitung schädlichen Datenverkehrs, beim Vorgehen gegen maliziöse Domains und bei der Abwehr bereits vorbereiteter Angriffe („Prepositioning“).²

Eine wirksame Abwehr schwerwiegender Cyberangriffe ist notwendig. Ebenso ist zu begrüßen, dass der Gesetzgeber hierfür ausdrückliche und technologisch auf die Besonderheiten des Cyberraums zugeschnittene Rechtsgrundlagen schaffen will. Der Entwurf geht dabei jedoch in

¹ BT-Drs. 21/6585, Seite 1.

² Vgl. BT-Drs. 21/6585, Seiten 1 f.

wesentlichen Punkten über das verfassungsrechtlich und sicherheitspolitisch Gebotene hinaus oder lässt erforderliche Sicherungen vermissen. Dies betrifft insbesondere die nur unzureichende richterliche und sonstige unabhängige Kontrolle eingriffsintensiver Maßnahmen, zu weit gefasste Gefahr- und Übermittlungsschwellen sowie unzureichende Vorgaben zum Schutz unbeteiligter Dritter und zur technischen Zuordnung von Angriffen. Hinzu kommen ungeklärte Zuständigkeits- und Koordinationsfragen zwischen Sicherheitsbehörden, eine problematische Verschiebung der Rolle des BSI von der zivilen Vertrauensstelle hin zu einer operativ handelnden Gefahrenabwehrbehörde sowie das Fehlen eines gesetzlichen Rahmens für den staatlichen Umgang mit bislang unbekannten Sicherheitslücken.

Ich rege daher an:

- für verdeckte Cyberabwehrmaßnahmen von erheblichem Grundrechtsgewicht eine vorherige unabhängige, regelmäßig richterliche Kontrolle vorzusehen und diese nicht auf Eingriffe in privat genutzte Systeme zu beschränken,
- Maßnahmen mit Drittbetroffenheit an zusätzliche Verhältnismäßigkeitsanforderungen zu knüpfen und Vorgaben zur Begrenzung von Kollateraleingriffen sowie zur Verlässlichkeit der technischen Zuordnung der Gefahrenquelle aufzunehmen,
- Offenbarungsverbote zeitlich zu begrenzen, frühzeitig einer gerichtlichen Kontrolle zu unterstellen und Geheimhaltungsentscheidungen zu Zwecken der Strafverfolgung den hierfür zuständigen Strafverfolgungsbehörden zuzuweisen,
- die Aufgabenzuweisung an das BKA in § 3a BKAG-E tatbestandlich enger zu fassen, klare Koordinations- und Abgrenzungsregeln gegenüber anderen Sicherheitsbehörden vorzusehen und Maßnahmen mit Auslandsbezug an besondere völkerrechtliche und verfahrensrechtliche Voraussetzungen zu knüpfen,
- die Eingriffsschwellen der §§ 68a ff. BKAG-E stärker nach dem Gewicht der jeweiligen Maßnahme zu differenzieren und die Übermittlung personenbezogener Daten an die Bundeswehr an qualifizierte Voraussetzungen und klare Zweckbindungen zu binden,
- für technisch eingriffsintensive Maßnahmen verbindliche Anforderungen an Prüfung, Freigabe und Absicherung der eingesetzten Mittel vorzusehen und das BSI bei Maßnahmen nach §§ 68c und 68d BKAG-E verbindlich in die technische Prüfung einzubeziehen,
- die Funktion des BSI als zivile Vertrauens- und IT-Sicherheitsstelle durch engere Übermittlungsschwellen, klare Zweckbindungen und unabhängige Kontrolle abzusichern sowie die Speicherung personenbezogener Sinkhole-Daten auf das Erforderliche zu begrenzen,
- ein gesetzlich geregeltes Schwachstellenmanagement für Zero-Day-Exploits einzuführen, das insbesondere Offenhalten, Nutzung, Beschaffung und Offenlegung bislang unbekannter Sicherheitslücken einem dokumentierten und überprüfbaren Abwägungsverfahren unterstellt.

Zu den Punkten im Einzelnen:

I. Artikel 1 Nummer 2 des Cybersicherheitsstärkungsgesetzes: § 41a BPolG-E

§ 41a BPolG-E schafft weitreichende Befugnisse der Bundespolizei zur technischen Abwehr von Cyberangriffen, lässt dabei jedoch zentrale grundrechtliche und verfahrensrechtliche Sicherungen offen.

Dies betrifft die nur punktuell vorgesehene richterliche Kontrolle besonders eingriffsintensiver Maßnahmen (vgl. 1.), die nur unzureichend begrenzte Betroffenheit unbeteiligter Dritter und das Fehlen hinreichender Vorgaben zur Vermeidung von Kollateraleingriffen und Fehlzuordnungen (vgl. 2.). Zudem kann das weitreichende Offenbarungsverbot Betroffene über längere Zeit von der Kenntnis der Maßnahme und damit von effektivem Rechtsschutz fernhalten (vgl. 3.).

1. Unzureichende richterliche Kontrolle

Der Entwurf unterstellt nur einen eng begrenzten Teil der in § 41a BPolG-E vorgesehenen verdeckten Cyberabwehrmaßnahmen einer vorherigen richterlichen Kontrolle. Dies trägt dem Gewicht der ermöglichten Grundrechtseingriffe nicht hinreichend Rechnung.

Die Entwurfsbegründung stellt für die Erforderlichkeit eines Richtervorbehalts maßgeblich darauf ab, dass es sich bei den Maßnahmen um Gefahrenabwehr und nicht um Überwachung handelt.³ Deshalb seien grundsätzlich weder qualifizierte Schutzgüter noch ein Richtervorbehalt erforderlich.⁴ Qualifizierte Anforderungen gelten nur, wenn in private Systeme eingegriffen und Daten erhoben werden.⁵

Entscheidend sind verfassungsrechtlich jedoch insbesondere Heimlichkeit und Eingriffsgewicht der Maßnahme (vgl. a)). Zudem beschränkt § 41a Abs. 5 und 6 BPolG-E den Richtervorbehalt bei Eingriffen in informationstechnische Systeme auf „privat“ genutzte Systeme, obwohl diese Einschränkung hinter dem Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zurückbleibt (vgl. b)). Auch Eingriffe in nicht privat genutzte Systeme können erhebliche Grundrechtseingriffe darstellen, insbesondere in Art. 10 Abs. 1 GG sowie in Grundrechte der betroffenen natürlichen und juristischen Personen (vgl. c)). Schließlich bleibt die heimliche Umleitung und Aufzeichnung von Datenverkehr nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E ohne vorherige richterliche Kontrolle, obwohl sie in ihrer Eingriffsintensität einer Telekommunikationsüberwachung jedenfalls nahekommen kann (vgl. d)).

Änderungsvorschlag: Der Richtervorbehalt sollte nicht allein an die private Nutzung eines informationstechnischen Systems und die Ermöglichung einer Datenerhebung anknüpfen. Vielmehr sollte § 41a BPolG-E für verdeckte Maßnahmen von erheblichem Grundrechtsgewicht eine vorherige unabhängige, regelmäßig richterliche Kontrolle vorsehen. Dies sollte insbesondere Eingriffe in informationstechnische Systeme unabhängig von deren privater oder geschäftlicher Nutzung sowie die heimliche Umleitung und Aufzeichnung von Datenverkehr nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E erfassen.

a) Die Zielrichtung einer Maßnahme ist kein tauglicher Maßstab für den Richtervorbehalt

Ob eine Maßnahme als Überwachungsmaßnahme oder als Gefahrenabwehrmaßnahme bezeichnet wird, entscheidet nicht darüber, ob sie einer vorbeugenden richterlichen Kontrolle bedarf. Maßgeblich sind vielmehr die Heimlichkeit und das Gewicht des Eingriffs. Beides kann bei Eingriffen in informationstechnische Systeme von Grundrechtssubjekten ohne deren Wissen nach § 41a BPolG-E vorliegen. Hinzu kommt, dass sich Löschungen und Veränderungen nachträglich oft nicht mehr beseitigen lassen.

Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil

³ BT-Drs. 21/6585, Seite 47.

⁴ BT-Drs. 21/6585, Seite 47.

⁵ BT-Drs. 21/6585, Seite 47.

der Betroffene sonst ungeschützt bliebe.⁶ Zwar ist dem Gesetzgeber bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, ein Regelungsspielraum eingeräumt.⁷ Bei einem Grundrechtseingriff von so besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum aber dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist.⁸ Denn der Richtervorbehalt kann die Interessen der Betroffenen verfahrensrechtlich absichern, obwohl sie diese wegen der Heimlichkeit der Maßnahme nicht selbst wahrnehmen können („kompensatorische Repräsentation“).⁹ Der Eingriff in informationstechnische Systeme ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.¹⁰

Schon das staatliche Eindringen in ein IT-System bewirkt eine Integritätsverletzung, und zwar unabhängig von dem Überwachungsziel einer Maßnahme.¹¹ Es greift zu kurz, eine Maßnahme allein anhand ihrer Ziel- und Zwecksetzung grundrechtlich zu bewerten.¹² Das Bundesverfassungsgericht hat deshalb die Einordnung der Quellen-TKÜ als bloßes funktionales Äquivalent zur klassischen TKÜ aufgegeben.¹³ Die Entwurfsbegründung bewertet die Maßnahmen dennoch allein nach ihrem Zweck: Weil es sich um Gefahrenabwehrmaßnahmen handele, sei ein Richtervorbehalt grundsätzlich nicht erforderlich.¹⁴

Hinzu kommt, dass sich Eingriffe nach § 41a Abs. 1 Satz 1 Nummer 3 BPolG-E oft nicht rückgängig machen lassen. Veränderungen sind nach § 41a Abs. 4 Nummer 2 BPolG-E nur rückgängig zu machen, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht. Sind Daten gelöscht oder verändert, kann nachträglicher Rechtsschutz dies nicht mehr beseitigen. Umso mehr bedarf es einer vorbeugenden richterlichen Kontrolle.

b) Die Beschränkung auf „privat“ genutzte Systeme ist enger als das Grundrecht, auf das sie sich beruft

Nach dem Gesetzesentwurf ist ein Richtervorbehalt nur vorgesehen, wenn ein System als eigenes privat genutzt wird (§ 41a Abs. 6 Satz 1, Abs. 5 Satz 2, Abs. 1 Satz 1 Nummer 3 BPolG-E). Diese Beschränkung stützt der Entwurf auf die Rechtsprechung des Bundesverfassungsgerichts zum IT-Grundrecht.¹⁵ Diese Rechtsprechung trägt die Beschränkung jedoch nicht. Das Bundesverfassungsgericht knüpft den Schutz daran, dass ein System als eigenes genutzt wird, unabhängig davon, wofür das System genutzt wird.

Die Legaldefinition übernimmt damit weitgehend die Formel des Bundesverfassungsgerichts,¹⁶ wonach die Daten einen Einblick in wesentliche Teile der Lebensgestaltung oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen müssen.¹⁷ Die Einschränkung eines als eigenes „privat“ genutzten Systems findet sich in der Rechtsprechung des Bundesverfassungsgerichts jedoch nicht.

⁶ BVerfG, UrT. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 259.

⁷ BVerfG, UrT. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 259.

⁸ BVerfG, UrT. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 259.

⁹ BVerfG, UrT. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 258.

¹⁰ BVerfG, UrT. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 210.

¹¹ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 114.

¹² BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 120.

¹³ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 121.

¹⁴ BT-Drs. 21/6585, Seite 47.

¹⁵ BT-Drs. 21/6585, Seite 47.

¹⁶ BT-Drs. 21/6585, Seite 47.

¹⁷ BVerfG, UrT. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.¹⁸ Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.¹⁹ Zudem hat das Bundesverfassungsgericht festgestellt, dass das IT-Grundrecht anzuwenden ist, wenn auf Systeme zugegriffen wird, die personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Einblick in wesentliche Teile der Lebensgestaltung einer Person oder gar ein aussagekräftiges Bild der Persönlichkeit gewonnen werden kann.²⁰ Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden.²¹ Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen.²² Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.²³

„Eigene oder eigengenutzte“ IT-Systeme, die das Bundesverfassungsgericht als vom IT-System-Grundrecht geschützt ansieht,²⁴ sind nicht mit als eigene „privat“ genutzten IT-Systemen gleichzusetzen. Die Eigennutzung beschreibt das Verhältnis des Betroffenen zum System und ob er allein oder mit anderen Berechtigten selbstbestimmt darüber verfügt.²⁵ Das Merkmal „privat“ beschreibt dagegen den Zweck der Nutzung. Der Gesetzesentwurf fügt damit eine zusätzliche Voraussetzung hinzu, die das Bundesverfassungsgericht nicht aufgestellt hat. Im Gegenteil hat es klargestellt, dass sich nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen lässt.²⁶

Das Merkmal bringt außerdem erhebliche praktische Schwierigkeiten mit sich. Der Bundesrat hat zu Recht darauf hingewiesen, dass es sich häufig erst im Nachgang feststellen lässt, ob ein System privat oder geschäftlich genutzt wird.²⁷

c) Auch Eingriffe in nicht-private Systeme berühren Grundrechte

Die Beschränkung des Richtervorbehalts auf privat genutzte Systeme lässt außer Acht, dass auch Eingriffe in Unternehmenssysteme in Grundrechte eingreifen, und zwar sowohl in Grundrechte natürlicher als auch juristischer Personen. Die Entwurfsbegründung hält einen Richtervorbehalt nur bei privater Systemnutzung für notwendig, weil nur dann das IT-Grundrecht betroffen sei.²⁸

¹⁸ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 206.

¹⁹ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 206.

²⁰ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

²¹ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

²² BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

²³ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

²⁴ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 104; BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23, MMR 2026, 52 ff., Rn. 173.

²⁵ Vgl. BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 206.

²⁶ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 203.

²⁷ BT-Drs. 21/7406, Seite 2.

²⁸ BT-Drs. 21/6585, Seite 47; BT-Drs. 21/7406, Seite 5.

Ob das IT-Grundrecht auch juristischen Personen zusteht, ist bislang nicht abschließend geklärt.²⁹ Darauf kommt es aus zwei Gründen nicht an.

Erstens werden Unternehmenssysteme von Beschäftigten genutzt, deren Grundrechtsschutz nach der Rechtsprechung des Bundesverfassungsgerichts auch bei geschäftlicher Nutzung berührt sein kann, sofern sie das System allein oder zusammen mit anderen zur Nutzung berechtigten Personen nutzen (vgl. oben bereits b)).³⁰

Zweitens ist jedenfalls das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG betroffen, soweit die Bundespolizei Daten zur Kenntnis nimmt, die mithilfe von Telekommunikationstechnik über Distanz übertragen werden,³¹ beispielsweise durch Umleitung und Aufzeichnung des Datenverkehrs (§ 41a Abs. 1 Satz 1 Nummer 2 BPolG-E) oder durch einen kommunikationsbezogenen Zugriff auf ein Endgerät (§ 41a Abs. 1 Satz 1 Nummer 3 BPolG-E). Staatliche Stellen sollen sich keine Kenntnis von Inhalt und Umständen der über TK-Anlagen abgewickelten Kommunikationen verschaffen können.³² Vom Fernmeldegeheimnis geschützt sind nicht nur die individuelle Fernkommunikation mittels einer TK-Einrichtung, sondern auch andere mithilfe von TK-Techniken über Distanz transportierte Daten.³³ Das Fernmeldegeheimnis unterscheidet nicht zwischen privater und geschäftlicher Kommunikation.³⁴ Zu recht stellt auch der Bundesrat fest, dass Unternehmen durch heimliche Eingriffe in ihre IT-Infrastruktur in ihren Grundrechten beeinträchtigt sind.³⁵

d) Umleitung und Aufzeichnung nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E als Eingriff in das Fernmeldegeheimnis ohne richterliche Kontrolle

Die Umleitung und Aufzeichnung von Datenverkehr nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E greift jedenfalls dann in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG ein, wenn hierdurch über Telekommunikationsnetze transportierte personenbezogene oder potentiell persönlichkeitsrelevante Daten erfasst werden. Aufgrund der heimlichen Umleitung, Aufzeichnung und möglichen Auswertung laufender Datenströme weist die Maßnahme erhebliche Parallelen zu einer Telekommunikationsüberwachung auf. Gleichwohl sieht der Entwurf keine vorherige richterliche Kontrolle vor.

Da § 41a Abs. 1 Satz 2 und Abs. 6 BPolG-E den Richtervorbehalt allein für Maßnahmen nach § 41a Abs. 1 Satz 1 Nummer 3 BPolG-E vorsehen, bleibt die Umleitung und Aufzeichnung von Datenverkehr auch ohne Wissen der Betroffenen nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E ohne richterliche Kontrolle. Die Aufzeichnung des umgeleiteten Datenverkehrs dient nach der Gesetzesbegründung auch der Auswertung des Datenverkehrs.³⁶ Folgerichtig unterwirft der Entwurf § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E der Löschpflicht für erlangte personenbezogene Daten.³⁷

Nach der Rechtsprechung des Bundesverfassungsgerichts schützt Art. 10 Abs. 1 GG nicht nur die individuelle Kommunikation zwischen Menschen, sondern auch andere mittels Telekommunikationstechnik über Distanz transportierte Daten und insbesondere die Erfassung von Rohdatenströmen des Telekommunikationsverkehrs.³⁸ Dies gilt auch für automatisiert übermittelte Daten, etwa

²⁹ Eher bejahend Warg, in: Kipker, Cybersecurity, 2. Auflage 2023, Kapitel 18 Rn. 80.

³⁰ BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 206.

³¹ Vgl. BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 87.

³² BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 87.

³³ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 91.

³⁴ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 88.

³⁵ BT-Drs. 21/7406, Seite 2; diese Bemerkung bezog sich auf die Parallelvorschrift des § 68d BKAG-E, gilt jedoch für § 41a BPolG-E gleichermaßen.

³⁶ BT-Drs. 21/6585, Seite 45.

³⁷ BT-Drs. 21/6585, Seite 50.

³⁸ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 91.

im Rahmen von Datensynchronisierungen oder Back-ups.³⁹ Der Schutz hängt dabei nicht davon ab, ob der staatliche Zugriff technisch auf der Übertragungsstrecke oder durch einen kommunikationsbezogenen Zugriff auf ein Endgerät erfolgt.⁴⁰

Damit kann auch die Kommunikation zwischen einem kompromittierten Endgerät und einem Command-and-Control-Server dem Schutz des Art. 10 Abs. 1 GG unterfallen. Dies gilt umso mehr, als nach der Entwurfsbegründung die umgeleiteten Daten neben Steuerungsinformationen und IP-Adressen im Einzelfall auch weitere auf dem betroffenen System gespeicherte Informationen, etwa von Schadsoftware abgegriffene Zugangsdaten, enthalten können.⁴¹

Eine klassische Telekommunikationsüberwachung stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen schweren Grundrechtseingriff dar und bedarf grundsätzlich einer vorherigen unabhängigen, regelmäßig richterlichen Kontrolle.⁴² Die heimliche Umleitung und Aufzeichnung laufender Datenströme zu Analysezwecken nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E erreicht jedoch jedenfalls ein erhebliches Eingriffsgewicht, das dem einer TKÜ nahekommen kann. Vor diesem Hintergrund ist erklärungsbedürftig, weshalb der Entwurf die Maßnahme vollständig von einer vorherigen unabhängigen Kontrolle ausnimmt.

Die unmittelbare Parallelregelung im BKAG findet sich in § 68c Abs. 1 BKAG-E. Danach darf auch das Bundeskriminalamt Datenverkehr, von dem eine Gefahr ausgeht, auf eine vorgegebene Zieladresse umleiten und aufzeichnen, ohne dass die Betroffenen hiervon Kenntnis haben. Die Entwurfsbegründung stellt die neuen Cyberabwehrmaßnahmen den klassischen staatlichen Überwachungsmaßnahmen gegenüber und leitet aus ihrer abweichenden Zielrichtung ab, dass für sie grundsätzlich weder qualifizierte Schutzgüter noch ein Richtervorbehalt erforderlich seien.⁴³ Im Zusammenhang mit Eingriffen in private informationstechnische Systeme nach §§ 68d, 68e BKAG-E führt sie ergänzend aus, dass betroffene Inhaber kompromittierter Systeme regelmäßig in eine Bereinigung einwilligen würden, und grenzt dies von der Telekommunikationsüberwachung ab, bei der eine Einwilligung dem Zweck der Maßnahme zuwiderliefe.⁴⁴

Diese Erwägung vermag den Verzicht auf eine unabhängige Kontrolle der Umleitungs- und Aufzeichnungsbefugnis nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E jedoch nicht zu tragen. Denn die Vorschrift erlaubt die Maßnahme ohne Wissen der Betroffenen und setzt eine Einwilligung gerade nicht voraus. Auch bei Eingriffen in Opfersysteme ist eine vorherige Einwilligung keineswegs stets praktisch erreichbar. Die Begründung zu den Parallelbefugnissen des BKA beschreibt selbst Fallgestaltungen, in denen über einen polizeilich übernommenen Command-and-Control-Server Deinstallations- oder Update-Befehle an eine Vielzahl infizierter Endgeräte übermittelt werden.⁴⁵ Eine individuelle vorherige Einwilligung sämtlicher betroffener Inhaber wird in solchen Konstellationen regelmäßig nicht vorliegen.

Gleichwohl sieht der Entwurf für Maßnahmen nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E weder einen Richtervorbehalt nach § 41a Abs. 6 BPolG-E noch eine individuelle Benachrichtigung nach § 78 Abs. 1 Satz 1 BPolG in der Fassung von Artikel 1 Nummer 4 des Entwurfs noch eine spezifische Protokollierung nach § 85 BPolG in der Fassung von Artikel 1 Nummer 6 des Entwurfs vor.

³⁹ BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19, MMR 2026, 44 ff., Rn. 91.

⁴⁰ BVerfG, Ur. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff., Rn. 184.

⁴¹ BT-Drs. 21/6585, Seiten 64 f.

⁴² BVerfG, Ur. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 235; BVerfG, Ur. v. 2.3.2010 – 1 BvR 256/08 u.a., NJW 2010, 833 ff., Rn. 247.

⁴³ BT-Drs. 21/6585, S. 47; entsprechend für die Parallelbefugnisse des BKA Seiten 66 f.

⁴⁴ BT-Drs. 21/6585, Seiten 47 und 66 f.

⁴⁵ BT-Drs. 21/6585, Seiten 65 f.

Angesichts der möglichen Erfassung und Analyse laufender, auch personenbezogener Datenströme bedarf dieser Verzicht auf verfahrensrechtliche Sicherungen einer besonderen Rechtfertigung.

2. Drittbetroffenheit

Der Entwurf lässt Eingriffe zulasten unbeteiligter Dritter in einem Umfang zu, der weder hinsichtlich der Zahl der Betroffenen noch hinsichtlich der Intensität ihrer Beeinträchtigung näher begrenzt wird. § 41a Abs. 3 BPolG-E stellt allein darauf ab, dass die Drittbetroffenheit unvermeidbar ist. Besondere Schutzvorkehrungen sieht der Entwurf nur punktuell für Maßnahmen nach § 41a Abs. 1 Satz 1 Nummer 3 BPolG-E vor. Für Betriebsuntersagungen sowie die Umleitung, Einschränkung oder Unterbindung von Datenverkehr fehlen vergleichbare Vorgaben. Hinzu kommt, dass der Entwurf keine Anforderungen an die Verlässlichkeit der technischen Zuordnung eines Angriffs zu einem bestimmten System oder Datenverkehr normiert, obwohl gerade Fehlzusammenhänge zu erheblichen Eingriffen gegenüber tatsächlich Unbeteiligten oder selbst Geschädigten führen können.

Änderungsvorschlag: § 41a BPolG-E sollte die Zulässigkeit von Maßnahmen mit Drittbetroffenheit ausdrücklich an zusätzliche Verhältnismäßigkeitsanforderungen knüpfen. Erforderlich sind insbesondere Vorgaben zur Begrenzung von Zahl und Eingriffsintensität betroffener Dritter, technische und organisatorische Vorkehrungen zur Minimierung von Kollateraleingriffen sowie hinreichende Anforderungen an die Verlässlichkeit der Zuordnung des Angriffs vor Durchführung der Maßnahme. Eingriffe in informationstechnische Systeme sollten zudem ausdrücklich subsidiär gegenüber gleichermaßen geeigneten, weniger eingriffsintensiven Maßnahmen ausgestaltet werden.

Nach § 41a Abs. 3 BPolG-E dürfen die besonderen Abwehrmaßnahmen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Dritte sind nach der Entwurfsbegründung alle, die nicht Betroffene sind.⁴⁶ Betroffene sind die Betreiber oder Nutzer von Systemen, von denen eine Gefahr ausgeht oder für die selbst eine Gefahr besteht.⁴⁷ Als Beispiel für Dritte nennt die Begründung Unbeteiligte, über deren Systeme Datenverkehr geroutet wird.⁴⁸

Außer dem Merkmal der Unvermeidbarkeit enthält § 41a Abs. 3 BPolG-E keine Begrenzung für die Betroffenheit Dritter. Der Entwurf legt weder fest, wie viele Unbeteiligte eine Maßnahme treffen, noch, wie schwer diese Beeinträchtigung wiegen darf. Technische Vorkehrungen, die eine Maßnahme auf gefahrgegenständliche Daten beschränken, verlangt § 41a Abs. 4 Nummer 1 BPolG-E nur für Maßnahmen nach § 41a Abs. 1 Satz 1 Nummer 3 BPolG-E. Für die Untersagung des Betriebs nach Nummer 1 und die Umleitung, Einschränkung oder Unterbindung von Datenverkehr nach Nummer 2 fehlt eine solche Vorgabe. Bei der Umleitung muss sich die Bundespolizei lediglich mit dem Bundesamt für Sicherheit in der Informationstechnik ins Benehmen setzen (§ 41a Abs. 10 BPolG-E). Anforderungen an die Folgen für Dritte ergeben sich daraus nicht.

Das erscheint insbesondere im Cyberraum problematisch, weil Abwehrmaßnahmen hier häufig in die Breite wirken können und der Entwurf keine Folgenabschätzung verlangt. So trifft die Abschaltung eines Servers oder die Umleitung seines Datenverkehrs alle anderen Kundinnen und Kunden desselben Hosting- oder Cloud-Anbieters.

Hinzu kommt das Risiko einer fehlerhaften Zuordnung, das der Gesetzentwurf nicht adressiert. Alle Maßnahmen setzen voraus, dass von dem System oder dem Datenverkehr eine Gefahr

⁴⁶ BT-Drs. 21/6585, Seite 46.

⁴⁷ BT-Drs. 21/6585, Seite 46.

⁴⁸ BT-Drs. 21/6585, Seite 46.

ausgeht (§ 41a Abs. 1 Satz 1 Nummer 1 bis 3 BPolG-E). Angreifer können ihre Herkunft verschleiern, indem sie fremde Systeme als Zwischenstationen nutzen. Hält die Bundespolizei ein solches System für die Quelle des Angriffs, trifft die Maßnahme Personen, die selbst Opfer des Angriffs sind. Der Entwurf enthält jedoch keine Vorgaben dazu, wie verlässlich die Zuordnung sein muss, bevor die Bundespolizei in ein System eingreift.

Die besonderen technischen Risiken sprechen darüber hinaus dafür, intrusive Eingriffe in informationstechnische Systeme ausdrücklich subsidiär gegenüber weniger eingriffsintensiven Abwehrmaßnahmen auszugestalten. Kann ein Angriff oder Datenabfluss bereits durch die Einschränkung, Unterbindung oder Umleitung des schädlichen Datenverkehrs wirksam beendet werden, bedarf es regelmäßig keines weitergehenden Eingriffs in das informationstechnische System selbst, insbesondere keines Löschens oder Veränderns dort gespeicherter Daten.

Einen entsprechenden Subsidiaritätsgedanken enthält das geltende BKAG bereits für den verdeckten Eingriff in informationstechnische Systeme. Nach § 49 Abs. 1 Satz 3 BKAG darf eine solche Maßnahme nur durchgeführt werden, wenn sie für die Aufgabenerfüllung erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre. Eine vergleichbare ausdrückliche Ultima-Ratio-Vorgabe sollte auch für intrusive Cyberabwehrmaßnahmen nach § 41a Abs. 1 Satz 1 Nummer 3 BPolG-E und § 68d BKAG-E vorgesehen werden. Dies würde zugleich dem Risiko von Fehlzusordnungen und irreversiblen Auswirkungen auf fremde Systeme Rechnung tragen.

3. Offenbarungsverbot kann Betroffene zeitlich unbegrenzt von Rechtsschutz abhalten

§ 41a Abs. 11 BPolG-E ermöglicht es der Bundespolizei, gegenüber Betreibern informationstechnischer Systeme und zur Mitwirkung verpflichteten Diensteanbietern anzuordnen, dass eine besondere Abwehrmaßnahme gegenüber den Betroffenen nicht offenbart werden darf. Die Regelung ist in zweifacher Hinsicht zu weit gefasst. Zum einen fehlt es an einer wirksamen zeitlichen Begrenzung des Offenbarungsverbots, weil die gerichtliche Kontrolle erst zwölf Monate nach Beendigung der zugrunde liegenden Maßnahme einsetzt, diese Maßnahme selbst aber nicht zwingend befristet ist. Betroffene können dadurch auf unbestimmte Zeit an der Kenntnisnahme und damit an effektivem Rechtsschutz gehindert werden (vgl. a)). Zum anderen darf das Offenbarungsverbot auch aus Gründen der Strafverfolgung aufrechterhalten werden, obwohl insoweit nicht die strengeren verfahrensrechtlichen Sicherungen der Strafprozessordnung, insbesondere richterliche Kontrolle und Befristung, zur Anwendung kommen (vgl. b)).

Änderungsvorschlag: *Das Offenbarungsverbot sollte sowohl zeitlich als auch verfahrensrechtlich enger gefasst werden. Seine Dauer sollte unabhängig von der Dauer der zugrunde liegenden Maßnahme gesetzlich begrenzt und jede darüber hinausgehende Aufrechterhaltung einer frühzeitigen gerichtlichen Kontrolle unterstellt werden. Soweit die Geheimhaltung nicht mehr der Gefahrenabwehr, sondern der Strafverfolgung dient, sollte die Entscheidung hierüber der zuständigen Strafverfolgungsbehörde nach Maßgabe der strafprozessualen Vorschriften überlassen werden.*

a) Zeitlich und personell unbegrenztes Offenbarungsverbot

Die Bundespolizei kann gem. § 41a Abs. 11 Satz 1 BPolG-E anordnen, dass der Betreiber des informationstechnischen Systems oder der zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr Verpflichtete gegenüber den von der besonderen Abwehrmaßnahme Betroffenen die besondere Abwehrmaßnahme nicht offenbaren darf, solange die Offenbarung Zwecken der Gefahrenabwehr oder Strafverfolgung entgegensteht. Erst wenn das Verbot nicht binnen zwölf Monaten nach Beendigung der Maßnahme aufgehoben wird, bedarf seine weitere Aufrechterhaltung der gerichtlichen Zustimmung, § 41a Abs. 11 Satz 2 BPolG-E. Eine prinzipielle Begrenzung

der Dauer der Maßnahme ist nicht vorgesehen. Dies bedeutet, dass Betroffene auf unbestimmte Zeit nichts von der Maßnahme gegen sie erfahren und Rechtsschutz erwirken können.

Die Gesetzesbegründung hat dabei den Fall vor Augen, dass ein Hosting-Anbieter seinen Kunden, einen Angreifer, über die Untersagung des Serverbetriebs informiert.⁴⁹ Betroffene sind nach der Entwurfsbegründung auch die Betreiber und Nutzer von Systemen, für die selbst eine Gefahr besteht,⁵⁰ dazu gehören also auch die Opfer eines Angriffs. Kommuniziert ein Botnetz aus infizierten Routern privater Nutzerinnen und Nutzern mit einem Steuerungsserver unter einer bestimmten Domain, so kann die Bundespolizei den Anbieter nach § 41a Abs. 9 Satz 1 BPolG-E verpflichten, den Datenverkehr zu dieser Domain an ein polizeiliches Sinkhole umzuleiten.⁵¹ Dort kann sie den Datenverkehr nach § 41a Abs. 1 Satz 1 Nummer 2 BPolG-E aufzeichnen und insbesondere betroffene IP-Adressen erfassen.⁵² Deren Inhaberinnen und Inhaber sind Betroffene, weil für ihre Systeme eine Gefahr besteht.

Gleichzeitig besteht die Möglichkeit, dem Anbieter nach § 41a Abs. 11 Satz 1 BPolG-E untersagen, den Betroffenen die Maßnahme zu offenbaren. Zwar nennt die Gesetzesbegründung als Zweck des Sinkholes gerade die Benachrichtigung von Gefährdeten und Opfern.⁵³ Ein Ausschluss des Offenbarungsverbots für diesen Fall ist jedoch nicht vorgesehen. Ob und wann eine Benachrichtigung erfolgt, liegt bei der Bundespolizei.

b) Aufrechterhalten aus Gründen der Strafverfolgung

Das Offenbarungsverbot darf nach § 41a Abs. 11 Satz 1 BPolG-E auch aus Gründen der Strafverfolgung aufrechterhalten werden. Darüber entscheidet die Bundespolizei als Gefahrenabwehrbehörde selbst, und zwar ohne die Sicherungen, die das Strafverfahrensrecht für eine solche Geheimhaltung vorsehen würde.

So kann nach § 95a Abs. 6 Satz 1 StPO einer nicht beschuldigten Person verboten werden, eine Beschlagnahme gegenüber dem Beschuldigten und Dritten zu offenbaren. Das Verbot setzt eine Abwägung der Interessen der Beteiligten im Einzelfall voraus. Es gilt nur für die Dauer einer Zurückstellung der Benachrichtigung, die allein das Gericht anordnen darf, § 95a Abs. 2 Satz 1 StPO. Diese ist nach § 95a Abs. 2 Satz 2 und 3 StPO auf höchstens sechs Monate zu befristen und kann nur durch das Gericht um jeweils höchstens drei Monate verlängert werden.

§ 41a Abs. 11 BPolG-E verzichtet auf die Sicherungen eines Richtervorbehalts und einer Befristung. Soweit die Geheimhaltung der Strafverfolgung dient, sollte die Entscheidung darüber nach dem Vorbild von § 74 Abs. 2 Satz 3 BKAG der Strafverfolgungsbehörde nach den Vorschriften des Strafverfahrensrechts überlassen werden.

II. Artikel 3 des Cybersicherheitsstärkungsgesetzes: Änderung des Bundeskriminalamtsgesetzes

Die in §§ 68b bis 68f BKAG-E vorgesehenen Cyberabwehrbefugnisse entsprechen in wesentlichen Teilen den Befugnissen des § 41a BPolG-E. Die unter I. entwickelten Einwände zur unzureichenden richterlichen Kontrolle besonders eingriffsintensiver Maßnahmen (vgl. I.1), zur nur unzureichend begrenzten Drittbetroffenheit und zu fehlenden Vorgaben gegen Kollateraleingriffe und

⁴⁹ BT-Drs. 21/6585, Seite 50.

⁵⁰ BT-Drs. 21/6585, Seite 46.

⁵¹ BT-Drs. 21/6585, Seiten 44 f.

⁵² BT-Drs. 21/6585, Seite 45.

⁵³ BT-Drs. 21/6585, Seite 45.

Fehlzuordnungen (vgl. I.2) sowie zum weitreichenden Offenbarungsverbot (vgl. I.3) gelten deshalb für die Parallelregelungen des BKAG entsprechend.

Darüber hinaus weist die Neuregelung im BKAG eigenständige Probleme auf. Dies betrifft die teilweise weit gefasste Aufgabenzuweisung an das Bundeskriminalamt und die fehlende hinreichende Abgrenzung zu den Zuständigkeiten anderer Sicherheitsbehörden sowie bei Maßnahmen mit Auslandsbezug (vgl. 1.). Zudem differenziert § 68a BKAG-E die Gefahrenschwellen nicht durchgehend nach dem Eingriffsgewicht der jeweiligen Maßnahme und sieht zugleich eine weit gefasste Übermittlungspflicht an die Bundeswehr vor (vgl. 2.). Darüber hinaus fehlen für technisch besonders eingriffsintensive Maßnahmen hinreichend konkrete Vorgaben zur Prüfung und Absicherung der eingesetzten Mittel, zur verbindlichen Beteiligung des BSI und zur Verlässlichkeit der technischen Zuordnung der Gefahrenquelle (vgl. 3.).

1. Artikel 3 Nummer 3 des Cybersicherheitsstärkungsgesetzes: Aufgabenzuweisung in § 3a BKAG-E

§ 3a BKAG-E weist dem Bundeskriminalamt neue Aufgaben zur Abwehr von Gefahren durch Cyberangriffe zu, grenzt deren sachlichen und institutionellen Anwendungsbereich jedoch nicht hinreichend klar ab. Die tatbestandlichen Voraussetzungen bleiben teilweise weit und auslegungsbedürftig, insbesondere soweit die Zuständigkeit an die Funktionsfähigkeit von Bundesbehörden oder an mögliche außen- und sicherheitspolitische Auswirkungen anknüpft (vgl. a)). Zugleich fehlen hinreichend klare Abgrenzungs-, Koordinations- und Verantwortungsregeln für Fälle konkurrierender Zuständigkeiten von BKA, Bundespolizei, BSI, Landesbehörden, Nachrichtendiensten und Bundeswehr (vgl. b)). Schließlich soll die Aufgabenzuweisung nach der Entwurfsbegründung auch Maßnahmen erfassen, die von Deutschland aus in informationstechnische Systeme im Ausland eingreifen, ohne dass der Entwurf die hierfür maßgeblichen völkerrechtlichen Voraussetzungen und das Verfahren der erforderlichen außenpolitischen Abstimmung näher regelt (vgl. c)).

Änderungsvorschlag: § 3a BKAG-E sollte tatbestandlich enger und normenklarer gefasst werden. Erforderlich sind insbesondere präzisere Zuständigkeitsvoraussetzungen, verbindliche Koordinations- und Abgrenzungsregeln gegenüber anderen Sicherheitsbehörden und den Ländern sowie besondere Voraussetzungen für Maßnahmen mit Auslandsbezug. Für Eingriffe in informationstechnische Systeme im Ausland sollte zudem ein Verfahren vorgesehen werden, das die völkerrechtliche Zulässigkeit und die außenpolitischen Auswirkungen vor Durchführung der Maßnahme prüft und die hierfür zuständigen Ressorts einbindet.

a) Unscharfe Tatbestände

Die Begründung betont, es handele sich nicht um eine allgemeine Zuständigkeit für die polizeiliche Gefahrenabwehr gegen Cyberangriffe, sondern um eine punktuelle Aufgabenerweiterung.⁵⁴ Diese Begrenzung kommt im Normtext jedoch nicht durchgehend mit gleicher Bestimmtheit zum Ausdruck.

Eine qualifizierte Gefahrenschwelle enthält lediglich § 3a Abs. 1 Nummer 1 BKAG-E. Danach wird das Bundeskriminalamt im Rahmen internationaler Zusammenarbeit nur tätig, wenn die Gefahr „schwerwiegend“ ist. § 3a Abs. 3 BKAG-E konkretisiert diesen Begriff abschließend für diese Fallgruppe. Für die Zuständigkeiten nach § 3a Abs. 1 Nummer 2 und 3 BKAG-E fehlt eine entsprechende Qualifikation.

⁵⁴ BT-Drs. 21/6585, Seite 59.

§ 3a Abs. 1 Nummer 2 BKAG-E lässt vielmehr eine Gefahr genügen, die sich gegen die Funktionsfähigkeit einer Behörde oder Einrichtung des Bundes richtet. Die Entwurfsbegründung versteht dieses Merkmal zwar dahin, dass nicht jede Cybergefahr ausreichen soll, sondern nur eine solche, welche die betroffene Stelle derart beeinträchtigen kann, dass ihre Arbeitsfähigkeit bedroht ist.⁵⁵ Diese einschränkende Schwelle kommt im Wortlaut der Vorschrift jedoch nicht in gleicher Deutlichkeit zum Ausdruck.

Noch weiter gefasst ist § 3a Abs. 1 Nummer 3 BKAG-E. Danach genügt, dass sich Gefahren ihrer Art nach oder wegen der zu ihrer Abwehr erforderlichen Maßnahmen auf die Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft oder die Verteidigung „auswirken können“. Die Vorschrift verlangt weder eine qualifizierte Gefahr noch ein bestimmtes Gewicht der möglichen außen- oder sicherheitspolitischen Auswirkungen. Die Gesetzesbegründung nennt zwar gewichtige Konstellationen wie Angriffe einer fremden Macht, Maßnahmen gegen IT-Systeme im Ausland oder Angriffe auf Hersteller von Rüstungsgütern.⁵⁶ Diese Beschränkungen finden sich im Tatbestand jedoch nicht wieder. Gerade weil größere Cyberangriffe regelmäßig grenzüberschreitende oder sicherheitspolitische Bezüge aufweisen können, bedarf die bundesrechtliche Aufgabenzuweisung einer präziseren tatbestandlichen Eingrenzung.

b) Fehlende Regelung konkurrierender Zuständigkeiten

§ 3a Abs. 4 Satz 1 BKAG-E bestimmt, dass die Aufgaben und Befugnisse anderer Bundesbehörden unberührt bleiben. Auch die Zuständigkeiten der Länder bestehen fort. Ihnen gegenüber sieht § 3a Abs. 4 Satz 2 BKAG-E lediglich eine Benachrichtigungspflicht des Bundeskriminalamts vor. Der Entwurf schafft damit keine ausschließliche Zuständigkeit des BKA, sondern lässt parallele Zuständigkeiten verschiedener Sicherheitsbehörden ausdrücklich bestehen.

Unklar bleibt jedoch, wie diese Zuständigkeiten im konkreten Einsatzfall voneinander abzugrenzen und miteinander zu koordinieren sind. Dies betrifft insbesondere Überschneidungen mit der Bundespolizei und dem BSI sowie mit den für die allgemeine Gefahrenabwehr zuständigen Landesbehörden. Eine bloße Benachrichtigung der Länder beantwortet weder die Frage, welche Behörde die operative Federführung übernimmt, noch wie bei voneinander abweichenden Gefahreinschätzungen oder Maßnahmenentscheidungen zu verfahren ist.

Besonders deutlich wird das Problem bei Sachverhalten mit außen- und sicherheitspolitischem Bezug. Die Entwurfsbegründung nennt ausdrücklich Angriffe einer fremden Macht oder durch diese unterstützte Angriffe und stellt zugleich klar, dass die Zuständigkeit der Streitkräfte für die Verteidigung unberührt bleibt.⁵⁷ Damit können polizeiliche Cyberabwehr und militärische Verteidigung im selben Sachverhalt zusammentreffen. Die abstrakte Fortgeltung beider Zuständigkeiten ersetzt keine Regelung darüber, nach welchen Kriterien zwischen polizeilicher Gefahrenabwehr und Verteidigung abzugrenzen ist und wie im Überschneidungsfall die Entscheidungskompetenzen verteilt werden.

Entsprechendes gilt für Auslandssachverhalte mit nachrichtendienstlicher Relevanz. Auch insoweit lässt § 3a Abs. 4 BKAG-E die Aufgaben anderer Bundesbehörden unberührt, ohne das Verhältnis der operativen Gefahrenabwehr des BKA zur nachrichtendienstlichen Informationsgewinnung insbesondere des Bundesnachrichtendienstes näher zu bestimmen. Angesichts der

⁵⁵ BT-Drs. 21/6585, Seite 60.

⁵⁶ BT-Drs. 21/6585, Seite 60.

⁵⁷ BT-Drs. 21/6585, Seite 60.

unterschiedlichen Aufgaben, Befugnisse und Kontrollregime bedarf es jedenfalls klarer Koordinations- und Verantwortungsregelungen.

c) Maßnahmen mit Auslandswirkung

Besonders weitreichend ist § 3a Abs. 1 Nummer 3 BKAG-E im Hinblick auf Maßnahmen mit Auslandsbezug. Nach der Entwurfsbegründung sollen hiervon Maßnahmen erfasst werden, die von Deutschland aus durchgeführt werden, aber informationstechnische Systeme im Ausland betreffen.⁵⁸ Als Beispiel nennt sie das Verändern oder Löschen von Daten auf IT-Systemen der Angreifer.⁵⁹

Derartige Maßnahmen werfen völkerrechtliche Fragen auf. Staatliche Eingriffe in informationstechnische Systeme, die sich im Hoheitsgebiet eines anderen Staates befinden, können dessen territoriale Souveränität berühren.⁶⁰ Ob und unter welchen Voraussetzungen ein solcher Eingriff völkerrechtlich zulässig ist, ist nach der öffentlichen Diskussion noch ungeklärt und wenig bestimmt.⁶¹ Die Entwurfsbegründung erkennt die außenpolitische Dimension zwar an und führt hierzu aus, die bei Maßnahmen nach § 3a Abs. 1 Nummer 3 BKAG-E erforderlichen außen- und sicherheitspolitischen Abwägungen könnten nur durch den Bund vorgenommen werden, weil dieser über die erforderlichen Lageeinschätzungen verfüge und aufgrund seiner Zuständigkeit für die auswärtigen Angelegenheiten über mögliche außenpolitische Auswirkungen entscheiden könne.⁶² Der Gesetzestext bildet dieses Erfordernis jedoch verfahrensrechtlich nicht ab. Insbesondere ist weder eine Beteiligung des Auswärtigen Amtes noch eine sonstige ressortübergreifende Prüfung der völkerrechtlichen Zulässigkeit und außenpolitischen Folgen vor Durchführung einer Maßnahme vorgesehen.

Dies fällt auch im Vergleich mit § 3 Abs. 1 Satz 2 Nummer 28 BSIG auf. Danach gehört es zu den Aufgaben des BSI, mit nationalen Computer-Notfallteams oder gleichwertigen Stellen von Drittstaaten zu kooperieren und diese zu unterstützen. Für Einsätze des BSI in Drittstaaten bestimmt die Vorschrift, dass sie nicht gegen den Willen des Staates erfolgen dürfen, auf dessen Hoheitsgebiet die Maßnahme stattfinden soll. Zudem trifft die Entscheidung über einen solchen Einsatz das Bundesministerium des Innern im Einvernehmen mit dem Auswärtigen Amt, § 3 Abs. 1 Satz 2 Nummer 28 BSIG. Für polizeiliche Maßnahmen des BKA nach § 3a Abs. 1 Nummer 3 i.V.m. §§ 68a ff. BKAG-E, die bis zum Verändern oder Löschen von Daten auf informationstechnischen Systemen im Ausland reichen können, enthält der Entwurf demgegenüber weder ein Zustimmungserfordernis des betroffenen Staates noch eine entsprechende Beteiligung des Auswärtigen Amtes.

§ 68d BKAG-E begrenzt das Auslesen, Löschen und Verändern zwar auf gefahrgegenständliche Daten. Hierzu gehören nach § 68d Abs. 2 BKAG-E jedoch insbesondere Schadprogramme und sonstige informationstechnische Angriffswerkzeuge einschließlich Steuerungs- und Protokolldateien. Die materielle Beschränkung des Eingriffsgegenstands beantwortet daher nicht die vorgelagerte Frage, unter welchen völkerrechtlichen und verfahrensrechtlichen Voraussetzungen deutsche Polizeibehörden auf einem im Ausland belegenen informationstechnischen System tätig werden dürfen.

⁵⁸ BT-Drs. 21/6585, Seite 60.

⁵⁹ BT-Drs. 21/6585, Seite 60.

⁶⁰ Lahmann, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Auflage 2024, § 6, Rn. 42.

⁶¹ Lahmann, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Auflage 2024, § 6, Rn. 42.

⁶² BT-Drs. 21/6585, Seite 60.

2. Artikel 3 Nummer 9 des Cybersicherheitsstärkungsgesetzes: Befugnisse und Gefahrenschwelle in § 68a BKAG-E

§ 68a BKAG-E knüpft die neuen cyberspezifischen Befugnisse des Bundeskriminalamts an die allgemeine Schwelle einer im Einzelfall bestehenden Gefahr, ohne die Eingriffsvoraussetzungen durchgehend nach der Intensität der jeweiligen Maßnahme zu differenzieren. Qualifizierte Anforderungen gelten nur für einen begrenzten Teil der Eingriffe in private informationstechnische Systeme nach § 68e BKAG-E. Insbesondere die heimliche Umleitung und Aufzeichnung von Datenverkehr bleibt dagegen grundsätzlich an die einfache Gefahrenschwelle gebunden (vgl. a)). Daneben verpflichtet § 68a Abs. 4 BKAG-E das Bundeskriminalamt zur Übermittlung von im Rahmen der Cyberabwehr erlangten Informationen an die Bundeswehr bereits bei tatsächlichen Anhaltspunkten für eine Berührung von Verteidigungsaufgaben, ohne die Übermittlungsvoraussetzungen nach Herkunft und Eingriffsintensität der Daten näher abzustufen (vgl. b)).

Änderungsvorschlag: Die Eingriffsschwellen der §§ 68a ff. BKAG-E sollten nach Art und Gewicht der jeweiligen Maßnahme differenziert und für besonders eingriffsintensive Befugnisse an qualifizierte Gefahren für hinreichend gewichtige Rechtsgüter geknüpft werden. Für die Übermittlung an die Bundeswehr sollte § 68a Abs. 4 BKAG-E insbesondere bei Daten aus eingriffsintensiven Maßnahmen eine entsprechend qualifizierte Übermittlungsschwelle sowie eine normenklar begrenzte Zweckbindung für die weitere Verwendung vorsehen.

a) Einfache Gefahr als allgemeine Befugnischwelle

§ 68a Abs. 1 BKAG-E eröffnet dem Bundeskriminalamt für seine Aufgaben nach den §§ 3a und 5 bis 8 BKAG-E ein weitreichendes Bündel allgemeiner und cyberspezifischer Gefahrenabwehrbefugnisse. Hierzu gehören insbesondere die Untersagung des Betriebs informationstechnischer Systeme nach § 68b BKAG-E, die auch ohne Wissen der Betroffenen mögliche Einschränkung, Unterbindung, Umleitung und Aufzeichnung von Datenverkehr nach § 68c BKAG-E sowie das Auslesen, Löschen und Verändern gefahrgegenständlicher Daten nach § 68d BKAG-E. Befugnisrechtliche Grundvoraussetzung ist nach § 68a Abs. 1 und 2 BKAG-E grundsätzlich lediglich eine im Einzelfall bestehende Gefahr der Verwirklichung einer der in § 3a Abs. 2 BKAG-E bezeichneten Straftaten.

Von dieser allgemeinen Gefahrenschwelle ist die vorgelagerte Aufgabenzuweisung zu unterscheiden. Nimmt das BKA eine Aufgabe nach § 3a BKAG-E wahr, müssen zusätzlich die dort geregelten Voraussetzungen des § 3a Abs. 1 BKAG-E erfüllt sein. Insbesondere verlangt § 3a Abs. 1 Nummer 1 i.V.m. Abs. 3 BKAG-E für die internationale Zusammenarbeit eine schwerwiegende Gefahr. § 68a Abs. 2 BKAG-E selbst erhöht die Eingriffsschwelle für die anschließende Ausübung der einzelnen Befugnisse jedoch nicht. Die Entwurfsbegründung stellt ausdrücklich klar, dass dieser Gefahrbegriff für sämtliche cyberspezifischen Befugnisse des Abschnitts 8a gilt, unabhängig davon, aufgrund welcher gefahrenabwehrrechtlichen Aufgabe das BKA tätig wird.⁶³

Eine qualifizierte materielle Eingriffsschwelle sieht erst § 68e Abs. 1 BKAG-E vor. Sie gilt jedoch ausschließlich für Maßnahmen nach § 68d BKAG-E, die ohne Einwilligung der Betroffenen durch einen Eingriff in ein privates informationstechnisches System eine Datenerhebung ermöglichen. Nur in diesen Fällen verlangt der Entwurf eine dringende Gefahr für besonders gewichtige Rechtsgüter. Für die Betriebsuntersagung nach § 68b BKAG-E, die heimliche Umleitung und Aufzeichnung von Datenverkehr nach § 68c BKAG-E sowie für Eingriffe nach § 68d BKAG-E, die nicht unter

⁶³ BT-Drs. 21/6585, Seite 63. Die Entwurfsbegründung stellt ausdrücklich fest, dass der Gefahrbegriff für alle cyberspezifischen Befugnisse nach Abschnitt 8a gilt.

die besonderen Voraussetzungen des § 68e Abs. 1 BKAG-E fallen, verbleibt es dagegen bei der allgemeinen Gefahrenschwelle.

Dies begegnet jedenfalls bei eingriffsintensiven Maßnahmen verfassungsrechtlichen Bedenken. Besonders tiefgreifende heimliche Überwachungsmaßnahmen dürfen nicht unterschiedslos zur Abwehr jeder Gefahr eingesetzt werden, sondern sind auf den Schutz hinreichend gewichtiger Rechtsgüter und entsprechend qualifizierte Gefahrenlagen zu begrenzen.⁶⁴ Vor diesem Hintergrund erscheint es nicht ausreichend, für Maßnahmen wie die heimliche Umleitung und Aufzeichnung laufender Datenströme oder intensive Eingriffe in informationstechnische Systeme grundsätzlich jede im Einzelfall bestehende Gefahr der Verwirklichung einer der in § 3a Abs. 2 BKAG-E aufgeführten Straftaten genügen zu lassen. Der Straftatenkatalog umfasst etwa auch § 263a StGB, ohne dass § 68a Abs. 2 BKAG-E nach der Schwere der konkret drohenden Tat oder dem Gewicht des bedrohten Rechtsguts differenziert.

b) Übermittlung an die Bundeswehr

§ 68a Abs. 4 BKAG-E verpflichtet das Bundeskriminalamt, Informationen, die im Zusammenhang mit der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik erlangt worden sind, unverzüglich an die Bundeswehr zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass Aufgaben der Verteidigung betroffen sind. Die Vorschrift erfasst ihrem Wortlaut nach sämtliche im Rahmen der Cyberabwehr erlangten Informationen und differenziert weder nach der Art ihrer Erhebung noch nach deren Eingriffsintensität. Damit können grundsätzlich auch personenbezogene Daten erfasst sein, die durch die heimliche Umleitung und Aufzeichnung von Datenverkehr nach § 68c BKAG-E oder durch Eingriffe in informationstechnische Systeme nach §§ 68d, 68e BKAG-E gewonnen wurden.

Die Übermittlung personenbezogener Daten an eine andere staatliche Stelle begründet nach der Rechtsprechung des Bundesverfassungsgerichts einen eigenständigen Grundrechtseingriff.⁶⁵ Werden die Daten bei der empfangenden Stelle zu einem gegenüber ihrer Erhebung geänderten Zweck verwendet, richtet sich die Zulässigkeit nach den verfassungsrechtlichen Anforderungen an eine Zweckänderung.⁶⁶ Bei Daten aus eingriffsintensiven Maßnahmen ist insbesondere das Kriterium der hypothetischen Datenneuerhebung maßgeblich, wonach die neue Nutzung dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen muss, dass diese eine Neuerhebung der Daten mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten.⁶⁷

§ 68a Abs. 4 BKAG-E knüpft die Übermittlung demgegenüber allein an tatsächliche Anhaltspunkte dafür, dass die Aufgaben der Verteidigung betroffen sind. Eine weitere Qualifikation nach Gewicht oder Konkretisierung der berührten Verteidigungsbelange enthält die Vorschrift nicht. Ebenso wenig differenziert sie danach, ob die zu übermittelnden Informationen durch geringfügige oder besonders eingriffsintensive Maßnahmen erlangt wurden. Damit fehlt gerade für Daten aus Maßnahmen nach §§ 68c bis 68e BKAG-E eine ausdrückliche Abstufung der Übermittlungsvoraussetzungen nach dem Gewicht des ursprünglichen Grundrechtseingriffs.

Hinzu kommt, dass § 68a Abs. 4 BKAG-E selbst die weitere Verwendung der übermittelten Informationen durch die Bundeswehr nicht näher begrenzt. Die Vorschrift bestimmt weder einen

⁶⁴ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 111.

⁶⁵ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 277.

⁶⁶ Vgl. BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 277.

⁶⁷ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 288.

konkreten Verwendungszweck noch differenziert sie nach Herkunft und Eingriffsgewicht der Daten. Gerade soweit Informationen aus heimlichen oder besonders eingriffsintensiven Maßnahmen betroffen sind, sollte die Übermittlung daher an eine nach dem Eingriffsgewicht abgestufte, hinreichend qualifizierte Schwelle geknüpft und die zulässige weitere Verwendung der Daten normenklar begrenzt werden.

3. Artikel 3 Nummer 9 des Cybersicherheitsstärkungsgesetzes: Technische Standards, BSI-Beteiligung und technische Zuordnung der Gefahrenquelle in § 68c Abs. 3 und § 68d Abs. 3 BKAG-E

Die neuen Cyberabwehrbefugnisse ermöglichen technisch weitreichende Eingriffe in Datenverkehr und informationstechnische Systeme, ohne das hierfür erforderliche technische Prüf- und Kontrollverfahren vollständig auszugestalten. Zwar enthält § 68d Abs. 3 BKAG-E einzelne Anforderungen an die Begrenzung und Absicherung eingesetzter Mittel. Verbindliche Vorgaben für deren Entwicklung, Prüfung und Freigabe fehlen jedoch (vgl. a)). Das BSI wird bei der Umleitung von Datenverkehr lediglich im Wege des Benehmens beteiligt und bei Eingriffen nach § 68d BKAG-E überhaupt nicht zwingend einbezogen, obwohl die Maßnahmen erhebliche Auswirkungen auf die allgemeine IT-Sicherheit haben können (vgl. b)). Schließlich knüpfen die Befugnisse an die technische Zuordnung einer Gefahr zu einem bestimmten System oder Datenverkehr an, ohne besondere Anforderungen an die Verlässlichkeit und Überprüfung dieser Zuordnung festzulegen (vgl. c)).

Änderungsvorschlag: *Der Entwurf sollte für technisch eingriffsintensive Cyberabwehrmaßnahmen verbindliche Anforderungen an Prüfung, Freigabe und Absicherung der eingesetzten Mittel sowie an die Verlässlichkeit der zugrunde liegenden technischen Zuordnung vorsehen. Das BSI sollte bei Maßnahmen nach §§ 68c und 68d BKAG-E aufgrund seiner besonderen technischen Fachkompetenz verbindlich beteiligt werden. Bei Maßnahmen mit erheblichen Auswirkungen auf die IT-Sicherheit sollte grundsätzlich sein Einvernehmen erforderlich sein oder jedenfalls eine Abweichung von seiner fachlichen Bewertung besonders begründet werden müssen.*

a) Unzureichende Vorgaben für technische Mittel und Verfahren

Nach § 68d Abs. 3 Satz 1 und 3 BKAG-E ist sicherzustellen, dass Veränderungen sich – soweit möglich – auf gefahrgegenständliche Daten beschränken und die vom BKA eingesetzten Mittel nach dem Stand der Technik gegen unbefugte Nutzung geschützt werden. Etwas strenger führt die Begründung aus, das BKA müsse die Mittel nach dem Stand von Wissenschaft und Technik schützen und sich der fortschrittlichsten technischen Verfahren bedienen.⁶⁸ Gleichwohl bleibt dieser Maßstab hinsichtlich der Fragen, wie die eingesetzten Werkzeuge zu entwickeln, zu testen und freizugeben sind, zu unbestimmt. Offen bleibt auch, ob zu den eingesetzten Mitteln die ausgenutzten Schwachstellen gehören (dazu unten IV.).

b) Benehmen mit dem BSI

Im Falle einer Anordnung zur Umleitung von Datenverkehr setzt sich das BKA nach § 68c Abs. 3 BKAG-E mit dem BSI ins Benehmen. Dies soll gewährleisten, dass beim BSI ein Gesamtüberblick über Umleitungsmaßnahmen bewahrt werden kann.⁶⁹ Das Anliegen, die Behörde mit der größten technischen Expertise einzubeziehen, ist zu begrüßen. Allerdings handelt es sich nicht um ein Einvernehmensrecht des BSI, sondern das Benehmen bedeutet, dass das BSI anzuhören ist und das

⁶⁸ BT-Drs. 21/6585, Seite 66.

⁶⁹ BT-Drs. 21/6585, Seite 65.

KA sich mit dessen Stellungnahme auseinandersetzt.⁷⁰ Zudem beschränkt § 68c Abs. 3 BKAG-E die Beteiligung auf die Umleitung von Datenverkehr. Für technisch mindestens ebenso sensible Eingriffe nach § 68d BKAG-E, insbesondere das Auslesen, Löschen oder Verändern von Daten in informationstechnischen Systemen, sieht der Entwurf keine entsprechende Beteiligung des BSI vor.

Dies überzeugt systematisch nur eingeschränkt. Der Gesetzgeber weist dem BSI gerade eine zentrale fachliche Verantwortung für die Sicherheit der Informationstechnik zu und erweitert mit demselben Gesetz dessen operative Aufgaben. Soweit Maßnahmen des BKA selbst Auswirkungen auf die Sicherheit informationstechnischer Systeme, unbeteiligte Dritte oder die allgemeine IT-Sicherheitslage haben können, sollte die technische Fachkompetenz des BSI verbindlich in das Entscheidungsverfahren einbezogen werden.

Denkbar wäre deshalb, für technisch besonders eingriffsintensive Maßnahmen nach §§ 68c und 68d BKAG-E das Benehmen durch ein Einvernehmen mit dem BSI zu ersetzen oder jedenfalls eine verbindliche fachliche Stellungnahme des BSI vorzusehen, von der das BKA nur unter besonders zu begründenden Voraussetzungen abweichen darf. Die Prüfung des BSI sollte sich dabei auf die Folgen für die IT-Sicherheit beschränken, insbesondere auf Risiken für unbeteiligte Systeme, die technische Beherrschbarkeit der Maßnahme, die Verlässlichkeit der Zuordnung der Gefahrenquelle und die etwaige Nutzung bislang unbekannter oder nicht geschlossener Sicherheitslücken. Die gefahrenabwehrrechtliche Letztverantwortung des BKA bliebe davon unberührt.

Zu den technischen Sicherungsvorgaben sollte ferner die Sicherheit der für die Maßnahme erforderlichen Kommunikations- und Übertragungswege gehören. Soweit Behörden oder verpflichtete Diensteanbieter im Rahmen der Cyberabwehr hochsensible technische Informationen über Schwachstellen, Angriffsmuster oder betroffene Systeme austauschen, kann bereits die hierfür geschaffene Übertragungsinfrastruktur selbst ein attraktives Angriffsziel darstellen. Der Entwurf sollte deshalb sicherstellen, dass auch solche behördlich veranlassten Datenflüsse durch angemessene technische und organisatorische Anforderungen nach dem Stand der Technik abgesichert werden.

c) Fehlende Anforderungen an die technische Zuordnung der Gefahrenquelle

Die Befugnisse der §§ 68b bis 68d BKAG-E setzen jeweils voraus, dass die abzuwehrende Gefahr einem bestimmten informationstechnischen System oder Datenverkehr technisch hinreichend zugeordnet werden kann. § 68b BKAG-E erlaubt die Untersagung des Betriebs eines Systems, „von dem“ die Gefahr ausgeht. Auch § 68c Abs. 1 BKAG-E knüpft an Datenverkehr an, „von dem“ die Gefahr ausgeht. Ebenso erlaubt § 68d Abs. 1 BKAG-E Eingriffe in das informationstechnische System, „von dem“ die Gefahr ausgeht.

Der Entwurf regelt jedoch nicht näher, welche tatsächliche und technische Erkenntnisgrundlage für diese Zuordnung erforderlich ist. Insbesondere enthält er keine besonderen Vorgaben zur Verlässlichkeit der technischen Identifizierung, zu einer unabhängigen fachlichen Überprüfung oder zu einem Mehraugenprinzip vor Durchführung besonders eingriffsintensiver Maßnahmen.

Dies ist gerade im Cyberraum von erheblicher Bedeutung. Angriffe können über kompromittierte Systeme unbeteiligter Dritter, Botnetze, Proxy-Infrastrukturen oder sonstige Zwischenstationen geführt werden. Ein System, von dem technisch Angriffsdatenverkehr ausgeht, muss daher nicht notwendig vom eigentlichen Angreifer betrieben werden. Die Entwurfsbegründung trägt diesem

⁷⁰ Vgl. Attendorn, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Auflage 2023, § 214 TKG, Rn. 14.

Umstand teilweise selbst Rechnung, indem sie ausdrücklich auch infizierte Opfersysteme und Botnetz-Infrastrukturen als Gegenstand der neuen Befugnisse beschreibt.⁷¹

Je schwerwiegender und weniger reversibel eine Maßnahme ist, desto höher sollten deshalb die Anforderungen an die Verlässlichkeit der technischen Zuordnung sein. Für Eingriffe nach §§ 68b bis 68d BKAG-E sollte der Gesetzgeber zumindest bei Maßnahmen von erheblichem Eingriffsge-
wicht besondere Anforderungen an die Dokumentation und Überprüfung der technischen Tatsa-
chengrundlage vorsehen. Bei besonders risikobehafteten Maßnahmen sollte zusätzlich eine fach-
liche Zweitprüfung, insbesondere unter Beteiligung des BSI, vorgesehen werden.

III. Artikel 2 des Cybersicherheitsstärkungsgesetzes: die Rolle und Befugnisse des BSI

Der Gesetzentwurf verändert die Stellung des BSI in mehrfacher Hinsicht. Zum einen erweitert er die Möglichkeiten, beim BSI vorhandene personenbezogene Daten für sicherheitsbehördliche, nachrichtendienstliche und militärische Zwecke weiterzugeben. Dies berührt die Funktion des BSI als vertrauenswürdige zivile Meldestelle und wirft Fragen der Zweckbindung und unabhängigen Kontrolle auf (vgl. 1.). Zum anderen weist der Entwurf dem BSI zusätzliche operative Eingriffsbe-
fugnisse gegenüber Kommunikations- und Netzinfrastrukturen zu und verschiebt damit sein Auf-
gabenprofil in Richtung einer eigenständig handelnden Gefahrenabwehrbehörde (vgl. 2.). Schließ-
lich verlängert § 16 Abs. 5 Satz 2 BSIG-E die Höchstspeicherdauer für Sinkhole-Daten von drei auf
24 Monate und vergrößert damit zugleich den Zeitraum, in dem personenbezogene Daten für wei-
tere sicherheitsbehördliche und nachrichtendienstliche Zwecke verfügbar bleiben (vgl. 3.).

Änderungsvorschlag: *Die Funktion des BSI als zivile, auf Prävention und technische IT-Sicher-
heit ausgerichtete Vertrauensstelle sollte institutionell und gesetzlich klarer abgesichert werden.
Übermittlungen personenbezogener Daten an Nachrichtendienste und Bundeswehr sollten insbe-
sondere bei eingriffsintensiv erhobenen Daten an qualifizierte Übermittlungsschwellen, klare
Zweckbindungen und wirksame unabhängige Kontrolle geknüpft werden. Operative Eingriffsbe-
fugnisse des BSI sollten auf das zur technischen Gefahrenabwehr Erforderliche begrenzt und mit
hinreichenden Rechtsschutz- und Schutzvorkehrungen versehen werden. Personenbezogene
Sinkhole-Daten sollten nur so lange gespeichert werden, wie ihre Personenbeziehbarkeit für die
Abwehrmaßnahme erforderlich ist. Für eine längerfristige technische Analyse sollten grundsätz-
lich anonymisierte oder jedenfalls hinreichend pseudonymisierte Daten verwendet werden.*

1. Das BSI als Vertrauensstelle

Das BSI nimmt nach § 5 Abs. 1 BSIG als zentrale Stelle Meldungen Dritter über Sicherheitsrisiken entgegen und ist zugleich nationaler Koordinator für die koordinierte Offenlegung von Schwach-
stellen nach Art. 12 Abs. 1 der NIS-2-Richtlinie. Diese Funktion setzt in besonderem Maße voraus,
dass Unternehmen, Sicherheitsforschende und sonstige Meldende darauf vertrauen können, dass
übermittelte Informationen zur Verbesserung der IT-Sicherheit und zur Schließung bestehender
Schwachstellen verwendet werden. Dem entspricht § 5 Abs. 3 BSIG, der das BSI grundsätzlich
verpflichtet, gemeldete Schwachstellen unverzüglich an den verantwortlichen Hersteller oder Pro-
duktverantwortlichen weiterzugeben, sofern sie nicht bereits öffentlich bekannt sind.

Auch das Bundesverfassungsgericht hat die organisatorischen und verfahrensrechtlichen Vorkeh-
rungen für den staatlichen Umgang mit bekannt gewordenen Sicherheitslücken als Bestandteil des
grundrechtlich gebotenen Schutzkonzepts für die Vertraulichkeit und Integrität

⁷¹ BT-Drs. 21/6585, Seiten 64 ff.

informationstechnischer Systeme eingeordnet.⁷² Die Stellung des BSI als vertrauenswürdige, auf die Stärkung der IT-Sicherheit ausgerichtete Fachbehörde ist deshalb nicht lediglich eine organisationspolitische Frage, sondern berührt die effektive Wahrnehmung staatlicher Schutzpflichten.

Das dem BSI entgegengebrachte Vertrauen gerät unter Druck, wenn Informationen, die dem BSI zu Zwecken der IT-Sicherheit übermittelt werden, zugleich für andere sicherheitsbehördliche oder militärische Zwecke verfügbar gemacht werden. Da auch das BSI dem Bundesministerium des Innern (BMI) untersteht, beaufsichtigt dasselbe Ministerium das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz, also Behörden mit einem operativen Interesse an Schwachstellenwissen. Dies verschärft die Notwendigkeit klarer gesetzlicher Zweckbindungen und institutioneller Sicherungen gegen eine funktionale Entgrenzung des beim BSI vorhandenen Schwachstellen- und Vorfallswissens.

Der Gesetzentwurf erweitert die bestehenden Übermittlungsmöglichkeiten erheblich. Nach § 8 Abs. 6 Satz 2 Nummer 3 BSIG-E kann das BSI personenbezogene Daten an den Bundesnachrichtendienst übermitteln, wenn Tatsachen einen internationalen kriminellen, terroristischen oder staatlichen Cyberangriff von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen. § 8 Abs. 6 Satz 2 Nummer 4 BSIG-E ermöglicht darüber hinaus die Übermittlung an die Bundeswehr bereits zur Unterrichtung über Tatsachen, die eine Bedeutung für die Erfüllung der Aufgaben der Verteidigung erkennen lassen.

Insbesondere die letztgenannte Tatbestandsschwelle in § 8 Abs. 6 Satz 2 Nummer 4 BSIG-E ist weit gefasst. Sie verlangt weder eine konkrete noch eine hinreichend konkretisierte Gefahr. Die bloße „Bedeutung“ einer Tatsache für Verteidigungsaufgaben lässt einen erheblichen prognostischen Spielraum. Da die Übermittlung an eine andere Stelle regelmäßig eine zweckändernde Nutzung personenbezogener Daten darstellt, bedarf sie einer eigenständigen grundrechtlichen Rechtfertigung.⁷³ Nach der Rechtsprechung des Bundesverfassungsgerichts muss insbesondere gewährleistet sein, dass die für die ursprüngliche Datenerhebung geltenden verfassungsrechtlichen Anforderungen nicht durch eine Weitergabe an andere Stellen unterlaufen werden.⁷⁴ Maßgeblich ist grundsätzlich, ob die Daten für den geänderten Zweck unter verfassungsrechtlich vergleichbar gewichtigen Voraussetzungen erneut erhoben werden dürften.⁷⁵

Hinzu kommt, dass § 5 Abs. 2 BSIG zwar grundsätzlich ermöglicht, Schwachstellen anonym zu melden oder die anonymisierte Weitergabe personenbezogener Daten zu verlangen, hiervon aber gerade für die Übermittlungsfälle des § 8 Abs. 6 und Abs. 7 Satz 1 BSIG eine Ausnahme macht. Es besteht damit für nicht anonym Meldende keine verlässliche Gewähr, dass ihre Identität gegenüber anderen Sicherheitsbehörden oder der Bundeswehr nicht offengelegt wird. Mit der Erweiterung des § 8 Abs. 6 BSIG-E erstreckt sich dieses Risiko zugleich auf die neu geschaffene Übermittlung an die Bundeswehr. Die Weiterverwendung personenbezogener Daten zu einem anderen als dem ursprünglichen Erhebungszweck stellt einen eigenständigen Grundrechtseingriff dar.⁷⁶ Sie ist deshalb insbesondere am Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie, soweit Telekommunikationsinhalte oder -umstände betroffen sind, an Art. 10 Abs. 1 GG zu messen.⁷⁷ Nach der Rechtsprechung des Bundesverfassungsgerichts bestimmt sich die Zulässigkeit einer solchen Zweckänderung bei eingriffsintensiv erhobenen Daten

⁷² BVerfG, Beschl. v. 8.6.2021 – 1 BvR 2771/18, NVwZ, 2021, 1361 ff., Rn. 65.

⁷³ BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15, NVwZ 2021, 226 ff., Rn. 97 ff.

⁷⁴ BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15, NVwZ 2021, 226 ff., Rn. 99.

⁷⁵ BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15, NVwZ 2021, 226 ff., Rn. 99.

⁷⁶ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 285 und 305.

⁷⁷ Vgl. BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 285.

grundsätzlich danach, ob die Daten für den neuen Zweck hypothetisch unter vergleichbar gewichtigen Voraussetzungen erneut erhoben werden dürften.⁷⁸

Besonders strenge Anforderungen gelten für Datenflüsse zwischen Behörden mit strukturell unterschiedlichen Aufgaben und Eingriffsbefugnissen. Für den Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten hat das Bundesverfassungsgericht ein informationelles Trennungsprinzip entwickelt.⁷⁹ Danach darf die unterschiedliche Ausgestaltung polizeilicher und nachrichtendienstlicher Erhebungsschwellen nicht dadurch unterlaufen werden, dass einmal erhobene Informationen ohne hinreichend qualifizierte Übermittlungsschwelle für die Aufgaben der jeweils anderen Behörde nutzbar gemacht werden.⁸⁰

Diese Problematik stellt sich im Entwurf insbesondere mit Blick auf den Bundesnachrichtendienst. Neben § 8 Abs. 6 Satz 2 Nummer 3 BSiG-E eröffnet auch § 8 Abs. 7 Satz 1 Nummer 4 BSiG-E eine Übermittlung an den BND, wenn tatsächliche Anhaltspunkte für den Verdacht bestimmter Straftaten bestehen und der Sachverhalt von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist. Während Übermittlungen nach § 8 Abs. 7 Satz 1 Nummer 1 und 2 BSiG-E an Strafverfolgungs- und Polizeibehörden einer vorherigen gerichtlichen Zustimmung bedürfen, genügt für Übermittlungen an Verfassungsschutzbehörden, MAD und BND nach Nummer 3 und 4 eine Anordnung des Bundesministeriums des Innern. Diese asymmetrische Kontrollarchitektur bedarf einer besonderen Rechtfertigung. Der BND verfügt über weitreichende Befugnisse zur strategischen und verdeckten Informationsgewinnung und ist gerade nicht an die für operative Gefahrenabwehr typischen Gefahrenschwellen gebunden. Werden Informationen aus einer zivilen IT-Sicherheitsbehörde in diesen Aufgabenbereich überführt, müssen Zweck, Anlass, Umfang und weitere Verwendung der Daten deshalb normenklar begrenzt sowie einer wirksamen unabhängigen Kontrolle unterstellt werden.⁸¹ Dass für eine Übermittlung an Nachrichtendienste lediglich eine ministerielle Anordnung vorgesehen ist, während bei bestimmten Übermittlungen an Polizei und Strafverfolgungsbehörden eine vorherige gerichtliche Kontrolle verlangt wird, erscheint vor diesem Hintergrund jedenfalls begründungsbedürftig.

2. Das BSI als operative Gefahrenabwehrbehörde

Parallel zu der Erweiterung der Datenübermittlungsbefugnisse verschiebt der Gesetzentwurf auch das Aufgabenprofil des BSI. Das Bundesamt soll nicht mehr lediglich beraten, warnen und technische Unterstützung leisten, sondern zunehmend selbst unmittelbar in Kommunikations- und Netzwerkinfrastrukturen eingreifen können und wird als Gefahrenabwehrbehörde im digitalen Raum beschrieben.⁸² Dies wirft zum einen Fragen nach Eingriffstiefe, Drittbetroffenheit und Rechtsschutz auf (vgl. a)), zum anderen nach der Bestimmtheit und technischen Absicherung neuer Informations- und Übermittlungspflichten (vgl. b)). Hinzu treten die Erweiterung der Befugnisse zum sogenannten Threat Hunting und die Frage, ob die bestehenden Transparenz- und Kontrollmechanismen der gewachsenen operativen Rolle des BSI noch angemessen Rechnung tragen (vgl. c)).

⁷⁸ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 ff., Rn. 287.

⁷⁹ BVerfG, Urt. v. 24.4.2013 – 1 BvR 1215/07, NJW 2013, 1499 ff., Rn. 123; BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15, GSZ 2021, 25 ff., Leitsatz 1.

⁸⁰ BVerfG, Urt. v. 24.4.2013 – 1 BvR 1215/07, NJW 2013, 1499 ff., Rn. 123; BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15, GSZ 2021, 25 ff., Leitsatz 1.

⁸¹ BVerfG, Urt. v. 19.5.2020 – 1 BvR 2835/17, NJW 2020, 2235 ff., Rn. 211 ff.

⁸² BT-Drs. 21/6585, Seite 28.

a) Operative Eingriffsbefugnisse und Rechtsschutz

So kann das BSI nach § 16a Abs. 1 BSIG-E gegenüber Top-Level-Domain-Registries und Domain-Name-Registry-Dienstleistern anordnen, Nameserver-Einträge zu verändern oder zu ergänzen, wenn dies zur Abwehr erheblicher Gefahren erforderlich ist. Nach § 16a Abs. 2 BSIG-E kann es zusätzlich die Umleitung von Nameserveranfragen auf einen vom BSI bestimmten Nameserver verlangen. § 17 BSIG-E erweitert daneben die Möglichkeiten, Anbieter digitaler Dienste in operative Maßnahmen zur Umleitung oder Unterbindung schädlichen Datenverkehrs einzubeziehen.

Damit nähert sich das BSI funktional einer Gefahrenabwehrbehörde an. Diese Entwicklung verändert die institutionelle Stellung des Bundesamtes und verschärft den Zielkonflikt zwischen seiner Rolle als kooperative Fach- und Meldestelle einerseits und seiner zunehmenden Eingriffsfunktion andererseits. Je stärker das BSI selbst hoheitliche Maßnahmen gegenüber Betreibern und Nutzern anordnet, desto weniger selbstverständlich ist, dass ihm Unternehmen und Sicherheitsforschende sensible Informationen in derselben Weise wie einer rein technisch-präventiv ausgerichteten Vertrauensstelle zur Verfügung stellen.

Die Maßnahmen können darüber hinaus grundrechtlich geschützte Positionen unbeteiligter Dritter berühren. Eine Umleitung von Nameserveranfragen oder Datenverkehr kann auch rechtmäßige Nutzer einer kompromittierten Domain, Kunden gemeinsam genutzter Infrastrukturen oder Betreiber erfassen, deren Systeme irrtümlich als Störquelle eingeordnet werden. Je nach technischer Ausgestaltung kommen neben dem Recht auf informationelle Selbstbestimmung insbesondere Art. 10 Abs. 1 GG sowie bei betroffenen Unternehmen Art. 12 Abs. 1 und Art. 14 Abs. 1 GG in Betracht. Der Gesetzgeber muss daher insbesondere sicherstellen, dass die Eingriffsvoraussetzungen hinreichend bestimmt sind, Maßnahmen auf das technisch Erforderliche begrenzt werden und effektive Rechtsschutz- und Kontrollmöglichkeiten bestehen.

Von besonderer Bedeutung ist insoweit auch die fehlende aufschiebende Wirkung von Widerspruch und Anfechtungsklage gegen Anordnungen nach § 16a Abs. 1 Satz 1 BSIG-E. Angesichts möglicher Fehlzurechnungen und erheblicher Auswirkungen einer Veränderung der Domainauflösung stellt sich daher auch die Frage, ob die vorgesehenen nachträglichen Rechtsschutzmöglichkeiten den Anforderungen des Art. 19 Abs. 4 GG in allen Konstellationen hinreichend Rechnung tragen.

b) Informations- und Übermittlungspflichten

Zusätzlicher Regelungsbedarf besteht bei den neu vorgesehenen Informations- und Übermittlungspflichten. § 15 Abs. 6 BSIG-E ermächtigt das BSI, von Anbietern öffentlich zugänglicher Telekommunikationsdienste und geschäftsmäßigen Anbietern digitaler Dienste Auskunft über sicherheitsrelevante technische Informationen zu verlangen. Der Entwurf konkretisiert dies zwar durch die Bezugnahme auf Schadaktivitäten, Schwachstellen, Verwundbarkeiten und aktuelle Bedrohungen (§ 15 Abs. 6 Satz 1 Nummer 1 bis 3 BSIG-E). Welche konkreten Datenkategorien hiervon erfasst werden und in welchem Detailgrad sie bereitzustellen sind, wird im Gesetz selbst jedoch nicht weiter bestimmt. Die Entwurfsbegründung nennt insoweit lediglich ergänzend Verkehrs- und Steuerungsdaten sowie technische Informationen, die von den Anbietern zur Verkehrsanalyse, Qualitätssicherung und aufgrund bestehender gesetzlicher Sicherheitsanforderungen verarbeitet werden.⁸³

⁸³ BT-Drs. 21/6585, Seiten 52 f.

Vergleichbares gilt für § 31 Abs. 3 Satz 1 Nummer 1 und 2 BSIG-E. Danach müssen Betreiber kritischer Anlagen automatisiert kontinuierliche Verfügbarkeitsindikatoren der für die Funktionsfähigkeit maßgeblichen informationstechnischen Systeme, Komponenten und Prozesse sowie Indikatoren zu tatsächlichen und potenziellen Angriffen und Informationen zu Schwachstellen übermitteln. Die näheren Anforderungen an Anbindung und Ausleitung soll das BSI nach § 31 Abs. 6 BSIG-E nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände festlegen und auf seiner Internetseite veröffentlichen. Angesichts der Sensibilität dieser Informationen sollte der Gesetzgeber die wesentlichen Kategorien der zu übermittelnden Daten und die Grenzen der Erhebung selbst hinreichend bestimmen.

Eine weitere technische Konkretisierung durch das BSI kann dabei sachgerecht sein. Denkbar wäre insbesondere eine gesetzlich vorgesehene Konkretisierung durch öffentliche Bekanntmachung. Der Gesetzgeber müsste jedoch selbst die wesentlichen Datenkategorien sowie Zweck, Gegenstand und Grenzen einer solchen Konkretisierungsbefugnis festlegen.⁸⁴ Dass eine derartige gestufte Regelung möglich ist, zeigt der Entwurf selbst für § 31 BSIG-E: Nach § 31 Abs. 3 BSIG-E bestimmt das Gesetz die zu übermittelnden Grundkategorien, während das BSI nach § 31 Abs. 6 BSIG-E die näheren Anforderungen an Anbindung und Ausleitung nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände festlegt und veröffentlicht

Besonders sicherheitsrelevant ist die in § 31 Abs. 3 BSIG-E vorgesehene kontinuierliche automatisierte Übermittlung von Daten kritischer Anlagen. Die Entwurfsbegründung führt hierzu aus, die Verfügbarkeitsindikatoren sollten als fortlaufende Zustandsanzeige, beispielsweise minütlich, an das BSI ausgeleitet werden.⁸⁵ Die Ausleitung soll automatisiert über eine gesicherte, unidirektionale und rückwirkungsfreie Verbindung erfolgen; die technischen Einzelheiten soll das BSI durch eine technische Richtlinie festlegen.⁸⁶ Der Entwurf erkennt damit selbst an, dass die neu geschaffene Verbindung technisch besonders abgesichert werden muss. Gleichwohl begründet jede dauerhafte technische Anbindung besonders sensibler Systeme einen zusätzlichen Kommunikationsweg, dessen Risiken eigenständig beherrscht werden müssen. Zusätzliche Außenverbindungen bei kritischen Anlagen können die Angriffsfläche vergrößern und die Zusammenführung detaillierter Verfügbarkeits- und Angriffsdaten selbst sicherheitsrelevante Informationen über die betroffenen Systeme erzeugen. Da beim BSI auf diese Weise Informationen über Verfügbarkeit, Angriffsindekatoren und Schwachstellen einer Vielzahl kritischer Anlagen zusammengeführt werden, wird der Schutzbedarf des dort entstehenden Datenbestands erhöht. § 31 BSIG-E sollte deshalb nicht nur Anforderungen an die Übermittlung selbst, sondern auch an Datenminimierung, technische Trennung, Zugriffsschutz und die Sicherheit der beim BSI aggregierten Datenbestände normenklar absichern.

c) Threat Hunting und nachträgliche Kontrolle

Die vorgesehene Erweiterung des § 11 BSIG auf Fälle des sogenannten Prepositionings bedarf demgegenüber zumindest einer klaren Abgrenzung vom geltenden Recht. Nach § 11 Abs. 1 BSIG kann das BSI bereits heute in herausgehobenen Fällen tätig werden, wenn die Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer erfassten Einrichtung beeinträchtigt ist. § 11 Abs. 1 BSIG-E soll das Tätigwerden nun ausdrücklich auch dann ermöglichen, wenn tatsächliche Anhaltspunkte für eine solche Beeinträchtigung vorliegen. Zugleich erweitert der Entwurf die Aufgabenbeschreibung in § 11 Abs. 1 Satz 1 Nummer 1 BSIG-E ausdrücklich um

⁸⁴ BVerfG, Urt. v. 19.5.2020 – 1 BvR 2835/17, NJW 2020, 2235 ff., Rn. 137 und 213 ff.

⁸⁵ BT-Drs. 21/6585, Seite 57.

⁸⁶ BT-Drs. 21/6585, Seiten 56 f.

die „Suche und Identifikation“ der Beeinträchtigung. Die Entwurfsbegründung ordnet hierzu bereits Vorbereitungshandlungen eines Angreifers als Beeinträchtigung der Sicherheit ein und nennt die systematische Suche nach Angreiferspuren als „Threat Hunting“.⁸⁷ Soweit damit lediglich klargestellt werden soll, dass ein bereits erfolgtes Eindringen ohne manifeste Funktionsbeeinträchtigung eine Beeinträchtigung der Sicherheit darstellen kann, sollte dies klar von einer materiellen Vorverlagerung der Befugnis abgegrenzt werden. Soweit dagegen bereits die Suche nach einer erst vermuteten Beeinträchtigung ermöglicht werden soll, liegt eine Erweiterung der bisherigen Eingriffslage vor, die eigenständig begründungsbedürftig ist.

Schließlich ist die Erweiterung operativer Befugnisse auch mit Blick auf ihre nachträgliche Kontrollierbarkeit zu betrachten. § 42 BSIG bestimmt gegenwärtig, dass Zugang zu Informationen und Akten in Angelegenheiten nach Teil 2 §§ 4 bis 10 und Teil 3 BSIG nicht gewährt wird. Lediglich die Akteneinsichtsrechte von Verfahrensbeteiligten bleiben unberührt. Die Vorschrift begründet damit für weite Teile der operativen Tätigkeit des BSI einen gesetzlichen Bereichsausschluss vom allgemeinen Informationszugang. Mit der Erweiterung der Eingriffs-, Anordnungs- und Datenverarbeitungsbefugnisse des BSI gewinnt zugleich die Frage an Gewicht, wie die fachlich-technischen Grundlagen ihrer Ausübung nachträglich nachvollzogen und kontrolliert werden können. Berechtigte Geheimhaltungsinteressen sprechen dabei nicht gegen jede Form von Transparenz, sondern für eine Regelung, die Informationszugang und Geheimschutz anhand der konkret betroffenen Informationen differenziert.

3. Verlängerung der Speicherdauer für Sinkhole-Daten

Besonders eingriffsintensiv ist schließlich die vorgesehene Verlängerung der Höchstspeicherdauer für sogenannte Sinkhole-Daten nach § 16 Abs. 5 Satz 2 BSIG-E von drei auf 24 Monate. Der Entwurf begründet die Verlängerung mit der technischen Komplexität von Cyberangriffen und dem hieraus resultierenden Analyseaufwand.⁸⁸

Die gespeicherten Datensätze können jedoch neben technischen Angriffsinformationen insbesondere IP-Adressen kompromittierter Systeme sowie weitere technische Merkmale enthalten, die Rückschlüsse auf betroffene Systeme und mögliche Einfallsvektoren erlauben. Die Verachtfa- chung der Höchstspeicherdauer bedarf deshalb einer eigenständigen Verhältnismäßigkeitsprüfung. Der pauschale Hinweis auf einen gesteigerten Analyseaufwand beantwortet noch nicht die Frage, weshalb personenbezogene oder personenbeziehbare Daten über den gesamten Zeitraum von 24 Monaten vorgehalten werden müssen. Soweit die Identifikation betroffener Systeme und die Benachrichtigung ihrer Nutzer abgeschlossen sind, ist insbesondere zu prüfen, ob die weitere Analyse nicht mit anonymisierten oder jedenfalls stärker pseudonymisierten technischen Daten durchgeführt werden kann.

Gegen die pauschale Verlängerung auf 24 Monate spricht zudem die unterschiedliche Funktion der anfallenden Sinkhole-Daten. Die Entwurfsbegründung erläutert, dass über Sinkholing insbesondere IP-Adressen kompromittierter Systeme identifiziert werden, um die Betroffenen über die jeweiligen Telekommunikationsanbieter warnen zu können. Daneben fallen technische Informationen etwa zu Schadprogrammen, betroffenen Systemen, Softwareständen, Hashwerten und möglichen Einfallsvektoren an.⁸⁹ Personenbezogene Identifikationsdaten einerseits und

⁸⁷ BT-Drs. 21/6585, Seite 52.

⁸⁸ BT-Drs. 21/6585, Seite 53.

⁸⁹ BT-Drs. 21/6585, Seiten 54 f.

längerfristig für die Angriffsanalyse relevante technische Erkenntnisse andererseits erfüllen damit unterschiedliche Funktionen. Dies spricht dafür, auch ihre Speicherdauer unterschiedlich zu behandeln.

Ist die Identifikation kompromittierter Systeme und die Benachrichtigung der Betroffenen abgeschlossen, bedarf es einer gesonderten Begründung dafür, weshalb die hierfür benötigten personenbezogenen Rohdaten weiterhin über einen Zeitraum von bis zu 24 Monaten gespeichert werden müssen. Das Bundesverfassungsgericht verlangt bei längerfristiger Speicherung grundrechtsrelevanter Daten normenklar geregelte Löschungspflichten und hinreichend engmaschige Prüfungen, die verhindern, dass Daten ohne fortbestehende Rechtfertigung gespeichert bleiben.⁹⁰ Technische Erkenntnisse über Angriffsmuster, Schadprogramme oder Einfallsvektoren können demgegenüber nach Entfernung des Personenbezugs weiterhin für die allgemeine Analyse von Cyberangriffen genutzt werden.

Auch der Vergleich mit § 8 Abs. 2 BStG spricht gegen eine undifferenzierte Höchstfrist von 24 Monaten. Protokolldaten der Kommunikationstechnik des Bundes dürfen danach längstens 18 Monate gespeichert werden und auch dies nur, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie zur Abwehr oder Erkennung von Schadprogrammen oder sonstigen erheblichen Gefahren erforderlich sein können. Für Daten, die länger als drei Monate gespeichert werden, verlangt § 8 Abs. 2 Satz 1 bis 3 BStG zudem tatsächliche Erkenntnisse über eine Betroffenheit des Bundes. Soweit automatisiert möglich, sind die Daten zu pseudonymisieren. Demgegenüber soll § 16 Abs. 5 Satz 2 BStG-E die gegenwärtige Höchstspeicherfrist für Sinkhole-Daten ohne weitere tatbestandliche Abstufung von drei auf 24 Monate verlängern.

Der rechtfertigend eingebrachte Analyseaufwand⁹¹ erklärt nicht, weshalb gerade personenbezogene Rohdaten während des gesamten Zeitraums verfügbar bleiben müssen. Sachnäher erscheint eine kürzere Grundfrist mit einer besonders zu begründenden Verlängerungsmöglichkeit für atypisch komplexe Angriffslagen. Jedenfalls sollte das Gesetz zwischen der Speicherung personenbezogener Rohdaten und der längerfristigen Speicherung anonymisierter technischer Erkenntnisse unterscheiden.

Die Verlängerung gewinnt außerdem zusätzliches Gewicht dadurch, dass § 16 Abs. 5 Satz 3 BStG-E auf die Übermittlungsregelungen des § 8 Abs. 6 und 7 BStG verweist. Der vergrößerte und länger verfügbare Datenbestand steht damit grundsätzlich auch für Übermittlungen an Strafverfolgungsbehörden, Polizeibehörden, Verfassungsschutzbehörden, den MAD, den BND und künftig die Bundeswehr zur Verfügung. Die Speicherdauer erhöht damit zugleich Umfang und zeitliche Reichweite eines Datenbestands, der für sicherheitsbehördliche und nachrichtendienstliche Sekundärzwecke nutzbar gemacht werden kann.

IV. Zero-Day-Exploits – Schwachstellenmanagement

Die Nutzung von dem Hersteller und den Nutzern unbekannten Sicherheitslücken durch staatliche Stellen begründet einen grundlegenden Zielkonflikt zwischen operativer Gefahrenabwehr und staatlicher IT-Sicherheitsvorsorge.

Änderungsvorschlag: *Der Entwurf sollte ein verbindliches Verfahren für den staatlichen Umgang mit bislang unbekannten Sicherheitslücken vorsehen. Insbesondere sollte gesetzlich geregelt werden, unter welchen Voraussetzungen Behörden Kenntnis von einer Schwachstelle zurückhalten*

⁹⁰ BVerfG, Urt. v. 19.5.2020 – 1 BvR 2835/17, NJW 2020, 2235 ff., Rn. 208.

⁹¹ BT-Drs. 21/6585, Seite 53.

und für eigene Maßnahmen nutzen dürfen und wann eine Offenlegung gegenüber dem Hersteller geboten ist. Dabei sollten insbesondere Verbreitungsgrad und Kritikalität der betroffenen Systeme, das Schadenspotenzial einer Ausnutzung durch Dritte, die Wahrscheinlichkeit einer unabhängigen Entdeckung, der Nutzen der Schwachstelle für den Schutz gewichtiger Rechtsgüter und die Verfügbarkeit milderer technischer Mittel berücksichtigt werden. Die Entscheidung sollte auf einer dokumentierten, behördenübergreifenden Abwägung der mit dem Offenhalten verbundenen Sicherheitsrisiken beruhen und regelmäßig überprüft werden. Zugleich sollten Beschaffung und Einsatz von Zero-Day-Exploits ausdrücklich geregelt und insbesondere der Erwerb auf nicht transparenten Exploit-Märkten an enge Voraussetzungen und wirksame Kontrolle gebunden werden.

Weiß der Staat von unbekannten Sicherheitslücken, verdichtet sich der allgemeine Schutzauftrag zu einer konkreten grundrechtlichen Verpflichtung, die Nutzerinnen und Nutzer informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren.⁹² Daraus folgt zwar keine ausnahmslose Verpflichtung, jede unbekannte Sicherheitslücke sofort und unbedingt dem Hersteller zu melden.⁹³ Wenn staatliche Behörden Schwachstellen in IT-Systemen jedoch bewusst offenhalten, um sie für eigene Eingriffe zu nutzen, geraten sie jedenfalls in Konflikt mit diesem Schutzauftrag. Das Bundesverfassungsgericht hat aus der grundrechtlichen Schutzpflicht abgeleitet, dass der Gesetzgeber den behördlichen Umgang mit Sicherheitslücken regeln muss.⁹⁴

Dem kommt der Entwurf nicht nach, denn er enthält hierzu keinerlei Regelung, noch wird die Problematik überhaupt adressiert. Es fehlt ein Vulnerability Equities Process nach dem Vorbild anderer Staaten, der eine strukturierte Abwägung zwischen dem Nutzen des Offenhaltens und dem Risiko einer Ausnutzung durch Dritte ermöglicht. Es werden keine Vorgaben zur Beschaffung von Schwachstellenwissen gemacht.

Vollständig ausgespart ist auch die Frage, ob Behörden Zero-Day-Exploits auf dem sogenannten „grauen Markt“ erwerben dürfen. Dort treten auch autoritäre Regime und kriminelle Akteure als Käufer auf und eine staatliche Nachfrage würde diesen Markt zusätzlich finanzieren.

Ein Gesetz, das staatlichen Behörden Befugnisse zum Eindringen in fremde IT-Systeme einräumt, ohne gleichzeitig den Umgang mit den dafür erforderlichen Schwachstellen zu regeln, weist eine strukturelle Lücke auf, die aus sicherheitspolitischer wie aus verfassungsrechtlicher Perspektive nicht hinnehmbar ist.

V. Gesamtergebnis

Der Gesetzentwurf verfolgt mit der Stärkung der staatlichen Handlungsfähigkeit gegenüber Cyberangriffen ein legitimes und angesichts der Bedrohungslage notwendiges Ziel. Die Schaffung ausdrücklicher Rechtsgrundlagen für technische Cyberabwehrmaßnahmen ist deshalb grundsätzlich zu begrüßen. In seiner gegenwärtigen Fassung hält der Entwurf die mit den neuen Befugnissen verbundenen grundrechtlichen, institutionellen und technischen Risiken jedoch nicht durchgehend durch entsprechend qualifizierte Eingriffsschwellen und verfahrensrechtliche Sicherungen ein.

Dies gilt zunächst für die neuen Befugnisse von Bundespolizei und BKA. Der Entwurf ermöglicht teilweise erhebliche und heimliche Eingriffe in informationstechnische Systeme und laufenden

⁹² BVerfG, Beschl. v. 8.6.2021 – 1 BvR 2771/18, NVwZ 2021, 1361 ff., Rn. 34.

⁹³ BVerfG, Beschl. v. 8.6.2021 – 1 BvR 2771/18, NVwZ 2021, 1361 ff., Rn. 43.

⁹⁴ BVerfG, Beschl. v. 8.6.2021 – 1 BvR 2771/18, NVwZ 2021, 1361 ff., Rn. 34 f.

Datenverkehr, ohne die vorherige richterliche Kontrolle konsequent am Gewicht des jeweiligen Grundrechtseingriffs auszurichten. Zugleich bleiben die Voraussetzungen für die Betroffenheit unbeteiligter Dritter, die technische Zuordnung einer Gefahrenquelle und die Geheimhaltung der Maßnahmen teilweise zu weit gefasst. Im BKAG kommen weit angelegte Aufgabentatbestände, ungeklärte Zuständigkeitsüberschneidungen und besondere Risiken bei Maßnahmen mit Auslandsbezug hinzu.

Auch die institutionelle Ausgestaltung bedarf der Nachschärfung. Die technische Fachkompetenz des BSI sollte bei besonders risikobehafteten Maßnahmen verbindlicher in die Entscheidung einbezogen werden. Zugleich darf die Erweiterung eigener Eingriffsbefugnisse und zusätzlicher Datenübermittlungen an Nachrichtendienste und Bundeswehr die Funktion des BSI als vertrauenswürdige zivile IT-Sicherheitsstelle nicht aushöhlen. Dies erfordert klare Zweckbindungen, qualifizierte Übermittlungsschwellen, unabhängige Kontrolle und eine auf das Erforderliche beschränkte Speicherung personenbezogener Daten.

Schließlich bleibt der staatliche Umgang mit bislang unbekannten Sicherheitslücken ungeregt. Gerade wenn Behörden künftig technische Befugnisse zum Eingriff in fremde IT-Systeme erhalten, muss der Gesetzgeber zugleich bestimmen, unter welchen Voraussetzungen Schwachstellen zurückgehalten, genutzt, beschafft oder gegenüber Herstellern offengelegt werden. Ohne ein transparentes und überprüfbares Schwachstellenmanagement besteht die Gefahr, dass operative Cyberabwehr und staatliche IT-Sicherheitsvorsorge in einen ungeregelten Zielkonflikt geraten.

Der Entwurf sollte daher vor seiner Verabschiedung insbesondere bei den Eingriffsschwellen, der richterlichen und fachlichen Kontrolle, der Begrenzung von Drittbetroffenheit und Datenweiterverwendung, der behördenübergreifenden Zuständigkeitsordnung sowie beim Schwachstellenmanagement nachgeschärft werden. Auf dieser Grundlage können die notwendigen Befugnisse zur Cyberabwehr geschaffen werden, ohne die hierfür ebenso notwendige rechtsstaatliche und technische Absicherung zurückzustellen.

Frankfurt am Main / Berlin, 01.10.2026

Prof. Dr. Dennis-Kenji Kipker
Research Director & CII-Founder