



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

Schriftliche Stellungnahme

von Prof. Dr. Dirk Heckmann, Technische Universität München vom
5. Oktober 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung der Cybersicherheit
BT-Drucksachen 21/6585, 21/7406

Gutachterliche Stellungnahme für den Innenausschuss des Deutschen Bundestages

Sachverständigen-Anhörung vom 05. Oktober 2026 zum

Gesetzesentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung der Cybersicherheit
BT-Drs. 21/6585

und der

Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung
BT-Drs. 21/7406

05. Oktober 2026

Univ.-Prof. Dr. Dirk Heckmann

Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München

Ass. iur. Nicolas Ziegler, wissenschaftlicher Mitarbeiter (TUM) und Geschäftsführer des
TUM CDPS

Ass. iur. Joanna Klauser, wissenschaftliche Referentin am
Bayerischen Forschungsinstitut für Digitale Transformation (bidt)

Zusammenfassung

Der Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (BT-Drs. 21/6585) ist im Grundsatz zu begrüßen und wird in weiten Teilen befürwortet. Cyberangriffe gefährden die Funktionsfähigkeit der Verwaltung, die Versorgungssicherheit und die wirtschaftliche Leistungsfähigkeit. Der Staat braucht wirksame Instrumente, um solche Angriffe frühzeitig zu erkennen und abzuwehren. Der Entwurf schließt hierfür wichtige Regelungslücken. Die in dieser Stellungnahme untersuchten Bereiche zeigen zugleich gezielten Nachbesserungsbedarf, um die neuen Befugnisse verfassungsrechtlich abzusichern.

Die Stärkung des BSI ist zu begrüßen

Die untersuchten Erweiterungen der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind rechtlich tragfähig und operativ sinnvoll. Sie verbessern die frühzeitige Erkennung verdeckter Angriffe, ermöglichen eine vorbeugende Unterstützung gefährdeter Einrichtungen und erweitern die Möglichkeiten, schädlichen Datenverkehr wirksam zu unterbinden oder umzuleiten. Die Einbeziehung von Domainverwaltung und modernen digitalen Diensteanbietern passt das Instrumentarium an die tatsächlichen Angriffswege an.

Auch die erweiterten Speicherbefugnisse sind unter den vorgesehenen Schutzvorkehrungen vertretbar. Zweckbindung, Zugriffsbeschränkungen und die Löschung nicht mehr erforderlicher Daten sichern die Verhältnismäßigkeit. Die Praxistauglichkeit der Eingriffsschwellen sollte nach Inkrafttreten evaluiert werden.

Die neuen Aufgaben des BKA brauchen klare Grenzen und Abstimmung

Die neuen Handlungsmöglichkeiten des Bundeskriminalamtes (BKA) bei der internationalen Cyberabwehr sind zu begrüßen. Sie ermöglichen insbesondere eine aktive Beteiligung an der Zerschlagung internationaler Botnetze und anderer Angriffsstrukturen. Die institutionelle Rollentrennung ist richtig: Das BSI bleibt zivile Schutz- und Beratungsinstitution; das BKA erhält die eingriffsintensiven Befugnisse für seine polizeilichen Aufgaben. Eine verbindliche Abstimmung zwischen beiden Behörden muss gesetzlich verankert werden.

Die Bundeskompetenzen in der polizeilichen Gefahrenabwehr sind begrenzt. Die Aufgaben und Befugnisse des BKA müssen konsequent auf die verfassungsrechtlich zulässigen Tätigkeiten des Bundes zugeschnitten werden. Insbesondere die Zuständigkeit zur Abwehr allgemeiner Cyberbedrohungen bedarf einer tatbestandlichen Begrenzung. Eine flächendeckende Cyberabwehrkompetenz des Bundes lässt sich auf diesem Weg nicht begründen. Die allgemeine polizeiliche Gefahrenabwehr bleibt Aufgabe der Länder.

Hackback braucht besondere gesetzliche Sicherungen

Aktive Zugriffe der Sicherheitsbehörden auf fremde IT-Systeme können in Ausnahmefällen zur Abwehr bestimmter Cyberangriffe erforderlich sein. Solche Befugnisse sind vertretbar, brauchen aber wegen ihrer besonderen Eingriffs- und Schadensrisiken präzise gesetzliche Grenzen. Im Vordergrund steht der Schutz unbeteiligter Dritter und bereits kompromittierter Opfersysteme.

Hackback muss ausdrücklich als letztes Mittel ausgestaltet werden. Erforderlich sind eine dokumentierte technische Folgenprüfung und eine belastbare Identifizierung des gefährverursachenden Systems. Die unvermeidbare Betroffenheit Dritter darf keinen Zugriff auf Verdacht rechtfertigen. Für besonders eingriffsintensive Maßnahmen sind höhere Gefahrenschwellen zu prüfen. Bei grenzüberschreitenden Zugriffen muss das Völkerrecht gewahrt bleiben.

Der staatliche Umgang mit bislang unbekannten Sicherheitslücken (Zero-Day-Schwachstellen) muss gesetzlich geregelt werden. Ein verbindliches Schwachstellenmanagement muss nach klaren Kriterien und innerhalb festgelegter Fristen über ihre operative Nutzung und die Benachrichtigung der Hersteller entscheiden. Die unbefristete Bevorratung solcher Lücken gefährdet die IT-Sicherheit der Allgemeinheit.

Der Grundrechtsschutz persönlichkeitsrelevanter IT-Systeme hängt nicht davon ab, ob sie privat oder beruflich genutzt werden. Die entsprechende Unterscheidung im Entwurf sollte aufgegeben werden. Richtervorbehalt und qualifizierte Schutzvorkehrungen müssen bei Eingriffen ohne wirksame Einwilligung auch für beruflich und gemischt genutzte Systeme gelten, die dem IT-System-Grundrecht unterfallen. Das gilt besonders für Opfersysteme.

Die vorgeschlagenen Nachbesserungen erhöhen die Rechtssicherheit der neuen Befugnisse und senken das Risiko einer späteren verfassungsgerichtlichen Korrektur. Damit sichern sie die staatliche Handlungsfähigkeit im Cyberraum und unterstützen das Ziel eines wirksamen Schutzes von Bürgern, Unternehmen und Verwaltung.

Inhalt der Stellungnahme

I.	Vorbemerkung.....	5
II.	Änderungen im BSIG.....	5
1.	Erweiterung der Speicherbefugnis in § 8 Abs. 2 BSIG-E.....	5
2.	Präventive Erweiterung der Befugnis des BSI nach § 11 BSIG-E	5
3.	Sinkholing nach § 16 Abs. 5 BSIG-E	6
4.	Erweiterung der Anordnungsbefugnisse zur Umleitung und Unterbindung von Schadverkehr (§§ 16a, 17 Abs. 2 BSIG-E)	6
5.	Befugnis zur Dekonnektierung von Domains nach § 16a Abs. 1 Satz 1 BSIG-E..	7
III.	Neue Kompetenzen im BKAG.....	8
1.	Abschnitt 8a und § 3a BKAG-E: Institutionelle Rollentrennung und Notwendigkeit gesetzlicher Abstimmungsmechanismen	8
2.	Institutionelle Rollentrennung	8
3.	Kompetenzrechtliche Einordnung: Spannungsverhältnis zwischen eng begrenzter Bundeskompetenz und weiter Befugnisarchitektur (§ 3a, Abschnitt 8a BKAG-E)	9
4.	Der strukturelle Widerspruch zu Abschnitt 8a BKAG-E	11
IV.	Besondere Abwehrmaßnahmen gemäß § 41a BPolG-E und §§ 68d, 68e BKAG-E – „Aktive Cyberabwehr“ („Hackback“)	11
1.	Grundsatz und Risikoprofil aktiver Abwehrmaßnahmen (§ 41a Abs. 1 S. 1 Nr. 3 BPolG-E, § 68d BKAG-E)	11
2.	Das staatliche Schwachstellen-Dilemma.....	13
3.	Empfehlung an den Gesetzgeber:	14
4.	Zurechnung und unvermeidbare Betroffenheit Dritter (§ 41a Abs. 3 BPolG-E, § 68d Abs. 4 BKAG-E)	14
5.	Klarstellungsbedarf.....	15
6.	Grundrechtliche Einordnung und Schutzniveau: Die verfehlte Differenzierung nach „privaten Systemen“ (§ 41a Abs. 1 S. 2, Abs. 5–8 BPolG-E, § 68e BKAG-E)	15
a)	Schutzbereich erfasst auch geschäftliche und gemischte Nutzung	16
b)	Kriterium der Eigennutzung statt pauschalem Ausschluss	16
c)	Opfersysteme als typischer Anwendungsfall.....	17
7.	Empfehlung	17

I. Vorbemerkung

Diese Stellungnahme beschränkt sich aufgrund der Kürze der Zeit zwischen der Benennung als Sachverständiger und der Anhörung am 5.10.2026 lediglich auf **ausgewählte Fragen**. Eine verfassungs- und sicherheitsrechtliche Begutachtung des gesamten Entwurfs ist damit nicht verbunden.

II. Änderungen im BSIG

Die vom Entwurf angestrebten Änderungen sollen übergeordnet der Schaffung neuer Möglichkeiten bzw. der Ergänzung bisheriger Möglichkeiten dienen, um groß angelegte Cyberangriffe unterbinden zu können.¹ Die hier begutachteten Änderungen im BSIG weisen **keine gewichtigen rechtlichen Bedenken** auf und vermögen **tatsächliche Verbesserungen** in der Arbeit des BSI zu bewirken. Ohne Anspruch auf Vollständigkeit der Bewertung des Entwurfs werden hier nur folgende Aspekte hervorgehoben:

1. Erweiterung der Speicherbefugnis in § 8 Abs. 2 BSIG-E

Die **Erweiterung der Speicherbefugnis** in § 8 Abs. 2 BSIG-E auf an den Schnittstellen der Kommunikationstechnik des Bundes anfallende Zeichenfolgen, die auf eine Ressource im Internet verweisen, etwa URLs, ist zu begrüßen. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG begegnen keinen Bedenken hinsichtlich der Verhältnismäßigkeit. Die Vorschrift sieht mehrere die Eingriffsintensität beschränkende Regelungen vor: wie etwa eine Pseudonymisierung, besondere Voraussetzungen für den Zugriff auf ältere Daten und dokumentierte Depseudonymisierung, ebenso eine Höchstspeicherfrist von 18 Monaten.

2. Präventive Erweiterung der Befugnis des BSI nach § 11 BSIG-E

Auch die **präventive Erweiterung der Befugnis des BSI, nach § 11 BSIG-E** in herausgehobenen Fällen auf Ersuchen der betroffenen Einrichtung, des betroffenen Betreibers oder einer anderen zuständigen Behörde Unterstützung leisten zu können, stellt eine wichtige Verbesserung in der Arbeit des BSI dar. Die Ausdehnung der Befugnis des BSI, nicht nur Maßnahmen zur Wiederherstellung der Sicherheit bzw. der Funktionsfähigkeit von IT-Systemen zu treffen, sondern auch „**Threat Hunting**“² **nach § 11 Abs. 1 Nr. 1 BSIG-E** betreiben zu können, ist zu begrüßen. Die notwendigen Anpassungen der erforderlichen Befugnis zur Verarbeitung der dabei entstehenden Daten nimmt der Entwurf vor.³

¹ BT-Drs. 21/6585, S. 1.

² BT-Drs. 21/6585, S. 52.

³ Vgl. Kemper, Cybergefahrenabwehrrecht, 2026, S. 268 ff.

Ob die Schwelle der „tatsächlichen Anhaltspunkte“ hierfür praxistauglich und sachgerecht ist, sollte im Rahmen einer späteren Evaluation geklärt werden. Es steht zu befürchten, dass hergebrachte sicherheitsrechtliche Eingriffsschwellen im Cyberraum ihre steuernde und begrenzende Funktion weitgehend einbüßen, da sich verdeckte Kompromittierungen einer verlässlichen tatbestandlichen Vorfeldprognose typischerweise entziehen.⁴

3. Sinkholing nach § 16 Abs. 5 BSIG-E

Auch die **Erhöhung der zulässigen Höchstspeicherdauer beim sog. Sinkholing nach § 16 Abs. 5 BSIG-E** von drei auf 24 Monate erweist sich bei verfassungsrechtlicher Gesamtwürdigung als tragfähig. Zwar markiert der Schritt von drei auf 24 Monate eine erhebliche zeitliche Ausweitung, die im Schrifttum und in der Praxis mit Blick auf Art. 10 Abs. 1 GG und das IT-System-Grundrecht nicht zu Unrecht aufmerksam hinterfragt wird. Allerdings erweist sich die bisherige Dreimonatsfrist angesichts der zeitlichen Dimension komplexer Cyberkampagnen und verdeckter ‚Schläfer‘-Infektionen operativ als vielfach unzureichend.

Der Eingriff bleibt verhältnismäßig: Die 24 Monate markieren eine strikte Höchstüberlassungsgrenze, keinen pauschalen Vorhaltezeitraum. Die Pflicht zur unverzüglichen Löschung greift weiterhin, sobald die Erforderlichkeit entfällt. Zudem federt der neu aufgenommene Verweis auf § 8 Abs. 6 und 7 BSIG die Eingriffsintensität wirksam ab, indem er strenge Zweckbindungs- und Übermittlungsschranken auch für diese Datenbestände verbindlich vorschreibt.

4. Erweiterung der Anordnungsbefugnisse zur Umleitung und Unterbindung von Schadverkehr (§§ 16a, 17 Abs. 2 BSIG-E)

Die Einführung der Befugnisse in **§ 16a BSIG-E** (gegenüber TLD-Registries wie der DENIC und Registraren) sowie in **§ 17 Abs. 2 BSIG-E** (gegenüber Diensteanbietern wie Cloud-Computing-, Hosting- und Content-Delivery-Network-Anbietern) schließen eine gravierende Regelungslücke des bisherigen Cybergefahrenabwehrrechts, wie der Entwurf richtig herausarbeitet.⁵ Bisher trafen Anordnungen zur Datenumleitung nach § 16 BSIG im Wesentlichen nur klassische Telekommunikations-Zugangsanbieter (Access-Provider). Dies griff jedoch operativ zu kurz:

- **Eingriff an der Quelle statt im Verteilerkreis (§ 16a BSIG-E):**

Wenn bösartige Domains für Command-and-Control-Server oder Phishing-Kampagnen genutzt werden, musste das BSI bislang versuchen, den Datenverkehr bei

⁴ Kemper, Cybergefahrenabwehrrecht, 2026, S. 104 et passim zur Eignung von Konzepten der Gefahrenabwehr gegenüber Cyberangriffen.

⁵ BT-Drs. 21/6585, S. 55.

einer Vielzahl einzelner Internetzugangsanbieter umzuleiten. Durch § 16a BSIG-E kann das BSI nun direkt an der Wurzel ansetzen – nämlich bei den Registry-Diensten und Registraren. Indem Nameserver-Einträge zentral modifiziert oder Anfragen direkt umgebogen werden, lässt sich die schädliche Namensauflösung flächendeckend und mit minimalem operativem Verzug neutralisieren.

- **Erfassung moderner Infrastrukturen (§ 17 Abs. 2 BSIG-E):**

Hochentwickelte Angreifer verteilen ihre Schadaktivitäten heute typischerweise über Cloud-Plattformen, DNS-Diensteanbieter oder Content-Delivery-Networks (CDNs), um herkömmliche Sperren zu umgehen. Die Erstreckung der Anordnungsbefugnis auf diese Akteure stellt sicher, dass das Gefahrenabwehrrecht mit den tatsächlichen Topologien des modernen Internets Schritt hält.

Die Neuregelungen sind auch verfassungsrechtlich verhältnismäßig ausgestaltet:

Hohe Eingriffsschwelle: Beide Vorschriften verlangen tatbestandlich das Vorliegen einer „*erheblichen Gefahr*“ für bedeutsame Schutzgüter (Sicherheit der Bundesnetze, kritische Infrastrukturen oder die Funktionsfähigkeit des Gemeinwesens).

Verhältnismäßigkeit im Einzelfall: Die Anordnungen stehen unter dem ausdrücklichen Vorbehalt der *technischen Realisierbarkeit* und der *wirtschaftlichen Zumutbarkeit* für die betroffenen Diensteanbieter.

Flankierender Rechtsschutz und Befristung: Durch den Verweis auf § 16 Abs. 5 BSIG-E gelten für anfallende Verkehrsdaten die dortigen strengen Schutz- und Zweckbindungsgarantien; zudem begründet § 16a Abs. 3 BSIG-E eine strikte Pflicht zur Beendigung der Maßnahme, sobald von dem Dienst keine Gefahr mehr ausgeht. Dass Widerspruch und Anfechtungsklage gemäß § 16a Abs. 1 Satz 2 BSIG-E keine aufschiebende Wirkung entfalten, ist angesichts der zeitkritischen Natur dynamischer Cyberangriffe sachgerecht und geboten.

5. Befugnis zur Dekonnektierung von Domains nach § 16a Abs. 1 Satz 1 BSIG-E

Die in **§ 16a Abs. 1 Satz 1 BSIG-E** geschaffene – und in der Entwurfsbegründung ausdrücklich als Möglichkeit zur Dekonnektierung von Domains erläuterte – Befugnis zur Anordnung der Änderung oder Ergänzung von Nameserver-Einträgen schließt eine wesentliche Lücke im Instrumentarium des BSI.

Kompetenzrechtlich begegnen die telekommunikations- und internetinfrastrukturbezogenen Eingriffsbefugnisse keinen Bedenken: Sie lassen sich auf die

gefahrenabwehrrechtliche Annexkompetenz zu Art. 73 Abs. 1 Nr. 7 Alt. 2 GG (Telekommunikation) stützen⁶, da die Maßnahmen strikt der Abwehr technischer Sicherheitsrisiken und Funktionsstörungen gewidmet sind und keine unzulässige, in die Kompetenz der Länder (Art. 70 GG) übergreifende Inhaltskontrolle bezwecken. Flankierend stützt sich der Bund für die Adressierung der Diensteanbieter zu Recht auf das Recht der Wirtschaft nach Art. 74 Abs. 1 Nr. 11 GG (BT-Drs. 21/6585, S. 24).

III. Neue Kompetenzen im BKAG

1. Abschnitt 8a und § 3a BKAG-E: Institutionelle Rollentrennung und Notwendigkeit gesetzlicher Abstimmungsmechanismen

Der vorgeschlagene neue Abschnitt 8a sowie § 3a BKAG-E werfen grundlegende Fragen der nationalen Cybersicherheitsarchitektur auf. Mit den vorgesehenen Befugnissen zur aktiven Cyberabwehr wird das Bundeskriminalamt neben dem BSI noch deutlicher als eigenständige Säule der operativen Cybergefahrenabwehr des Bundes konturiert.⁷

Gegen diese Ausgestaltung wird eingewandt, sie verstärke die ohnehin beklagte horizontale Komplexität und Zersplitterung der deutschen Cybersicherheitslandschaft, wo vielmehr eine Bündelung und Komplexitätsreduktion geboten wäre. Dieser Einwand greift im Ergebnis jedoch zu kurz. Das BKA verfügt bereits nach geltendem Recht über gewichtige gefahrenabwehrrechtliche und strafprozessuale Zuständigkeiten im Cyberraum⁸, sodass hier kein sachfremder Bruch vorliegt.

2. Institutionelle Rollentrennung

Vor allem aber ist die **strikte institutionelle Rollentrennung verfassungs- und sicherheitspolitisch ausdrücklich zu begrüßen:**

- **Wahrung des defensiven Vertrauensprimats des BSI:**

Das BSI erfüllt seine Funktion als zivile Schutz- und Beratungsinstitution für Wirtschaft, Bürger und Verwaltung nur dann wirksam, wenn es als neutraler und verlässlicher Partner wahrgenommen wird. Würden dem BSI hochintrusive Maßnahmen der aktiven Cyberabwehr übertragen, geriete die Behörde in einen unlösbaren strukturellen Zielkonflikt zwischen dem Schließen von Sicherheitslücken

⁶ Hierzu auch Uhle, in: Dürig/Herzog/Scholz, 110. EL März 2026, GG Art. 73 Rn. 175; Heintzen, in: Huber/Voßkuhle, 8. Aufl. 2024, GG Art. 73 Rn. 81; vgl. auch Poscher/Lassahn, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 7 Rn. 52.

⁷ So bereits für den Referentenentwurf Ziegler/Kemper, Das BKA als Cyberabwehrbehörde, VerfBlog v. 24.3.2026, abrufbar unter: <https://verfassungsblog.de/das-bka-als-cyberabwehr-behoerde/>.

⁸ Golla, in: Liskén/Denninger/Bäcker PolR-HdB, 8. Aufl. 2026, Kap. 8 Rn. 679 ff.

einerseits und deren operativer Offenhaltung oder Ausnutzung andererseits. Die Zuweisung eingriffsintensiver Befugnisse an die primär polizeilich geprägte Eingriffsverwaltung des BKA schützt das BSI vor diesem Glaubwürdigkeitsverlust und stärkt das Vertrauen in die präventive IT-Sicherheitsarchitektur.⁹

- **Regelungsdefizit: Erfordernis eines zwingenden Abstimmungsverfahrens:**
Die institutionelle Differenzierung darf im operativen Vollzug jedoch nicht zu Reibungsverlusten oder Gefahrenverlagerungen führen. Aktive Abwehrmaßnahmen des BKA bergen systemimmanent das Risiko von unvorhergesehenen Nebenwirkungen auf die Stabilität informationstechnischer Infrastrukturen oder von Kollisionen mit zeitgleich laufenden defensiven Maßnahmen des BSI (wie etwa Umleitungen nach §§ 16, 16a BSIG-E).

Im weiteren Gesetzgebungsverfahren sollte daher in § 3a BKAG-E bzw. im neuen Abschnitt 8a ein **gesetzliches Benehmensefordernis oder ein verbindlicher Koordinierungsmechanismus mit dem BSI** (beispielsweise unter institutionalisierter Nutzung des Nationalen Cyber-Abwehrzentrums) verankert werden. Nur durch eine gesetzlich festgeschriebene Pflicht zur Lageabstimmung im Vorfeld operativer Eingriffe lässt sich gewährleisten, dass aktive Maßnahmen des BKA die defensive Schutzwirkung für die zivilen Netze nicht konterkarieren.

3. Kompetenzrechtliche Einordnung: Spannungsverhältnis zwischen eng begrenzter Bundeskompetenz und weiter Befugnisarchitektur (§ 3a, Abschnitt 8a BKAG-E)

Die in Abschnitt 8a BKAG-E vorgesehenen Befugnisse sind vor allem im Lichte der bundesstaatlichen Kompetenzordnung kritisch zu beleuchten. Auch wenn das materielle Cybersicherheitsrecht in weiten Teilen bundesrechtlich geprägt ist¹⁰, verbleibt die allgemeine Gefahrenabwehr nach Art. 30, 70 Abs. 1 GG im Grundsatz bei den Ländern.¹¹ Das Grundgesetz weist dem Bund für eine originäre polizeiliche Gefahrenabwehr durch das BKA lediglich eng umrissene Ausnahmetitel zu – namentlich die Abwehr von Gefahren des internationalen Terrorismus (Art. 73 Abs. 1 Nr. 9a GG), die föderale Zentralstellenfunktion (Art. 73 Abs. 1 Nr. 10 lit. a GG) sowie die internationale Kriminalitätsbekämpfung (Art. 73 Abs. 1 Nr. 10 a.E. GG). Dass sich der Entwurf zur Begründung umfassender Eingriffsbefugnisse flankierend auf Art. 73 Abs. 1 Nr. 1 GG sowie auf eine ungeschriebene Kompetenz kraft Natur der Sache stützt (BT-Drs. 21/6585, Begründung A.III), vermag eine generelle Bundes-Cyberpolizei verfassungsrechtlich nicht zu tragen.

⁹ Umfassend zur Thematik bei *Ritter*, Int. Cybersec. L. R. 2025, 1 ff.

¹⁰ *Kemper*, Cybergefahrenabwehrrecht, 2026, S. 360 ff.

¹¹ *Amthor*, GSZ 2020, 251 (253 f.).

§ 3a BKAG-E mag insoweit im Grundsatz noch mit der Kompetenzordnung vereinbar sein, wenn man ihn **verfassungskonform auslegt**.

- **Zerschlagung internationaler Cybercrime-Infrastrukturen (§ 3a Abs. 1 Nr. 1 BKAG-E):**

Im Grundsatz lässt sich § 3a BKAG-E verfassungskonform handhaben, wenn man die Norm strikt an den engen verfassungsrechtlichen Ermächtigungen misst. Ein zentraler und praxisrelevanter Anwendungsfall des § 3a Abs. 1 Nr. 1 BKAG-E ist die Zerschlagung internationaler Botnetze und Cybercrime-Infrastrukturen („Takedowns“) im Verbund mit ausländischen Sicherheitsbehörden. Diese Alternative setzt schwerwiegende Gefahren voraus, deren Abwehr zwingend ein koordiniertes Vorgehen mit ausländischen oder überstaatlichen Stellen erfordert. Für diese genuine Schnittstelle internationaler Gefahrenabwehr schafft der Entwurf eine **be-
grüßenswerte Zuständigkeit** und mit Instrumenten wie § 68c BKAG-E sinnvolle Ermächtigungen, damit sich das BKA an solchen Operationen künftig auch technisch-aktiv beteiligen kann. Daneben enthält § 3a Abs. 1 Nr. 2 und 3 BKAG-E eigenständige Aufgabenalternativen.¹²

- **Terrorismusabwehr und Bundesverwaltung (§ 3a Abs. 1 Nr. 2 BKAG-E):**

Soweit Cyberangriffe mit terroristischem Bezug abgewehrt werden sollen, trägt Art. 73 Abs. 1 Nr. 9a GG die Regelung; der Schutz der Regierungsinfrastruktur lässt sich zudem auf die Organisationsgewalt des Bundes bzw. eine Kompetenz kraft Natur der Sache stützen.

- **§ 3a Abs. 1 Nr. 3 BKAG-E:**

Die Zuständigkeit des BKA für Cybergefahren mit außen- oder verteidigungspolitischen Bezug ist grundsätzlich nachvollziehbar. Präzisierungsbedürftig bleibt jedoch die Formulierung, dass sich die Gefahren oder die erforderlichen Abwehrmaßnahmen auf diese Bereiche „auswirken können“. Zur verfassungsgerichtlichen Absicherung sollte klargestellt werden, dass ein anhand konkreter Umstände nachvollziehbarer, hinreichend gewichtiger Bezug zu auswärtigen Angelegenheiten oder zur Verteidigung erforderlich ist. Ein bloßer Auslandsbezug der technischen Infrastruktur sollte hierfür nicht genügen.

¹² Ziegler/Kemper, Das BKA als Cyberabwehrbehörde, VerfBlog v. 24.3.2026, abrufbar unter: <https://verfassungsblog.de/das-bka-als-cyberabwehrbehorde/>.

4. Der strukturelle Widerspruch zu Abschnitt 8a BKAG-E

Bedenken weckt vor allem, dass Abschnitt 8a BKAG-E in seiner Gesamtheit keine eng begrenzte Spezialzuständigkeit abbildet, sondern eine **umfassende Zuständigkeit für die Cybergefahrenabwehr suggeriert**. Dies verdeutlicht insbesondere **§ 68a BKAG-E**, der ausweislich der Begründung eine „polizeiliche Generalklausel für die Cyberabwehr“¹³ darstellt. Zwar bindet § 68a Abs. 1 BKAG-E die Befugnisse formal an die Aufgaben nach §§ 3a und 5 bis 8 BKAG rück, sodass die Norm keine neuen Aufgaben schafft. Hinsichtlich der verfassungsrechtlich eng begrenzten Zuständigkeit des BKA einerseits und der Schaffung einer allumfassenden Gefahrenabwehrklausel andererseits besteht im Entwurf jedoch ein unübersehbarer Wertungswiderspruch: Das Rechtsinstitut einer polizeilichen Generalklausel ist das typische Instrument einer originären Landesvollzugspolizei, nicht das einer spezialisierten Bundeszentralstelle.

Es **empfiehlt** sich daher, die Befugnisse in Abschnitt 8a stärker auf den verfassungsrechtlich zulässigen Ausschnitt der Tätigkeiten des BKA im Cyberraum zuzuschneiden und klarzustellen, dass hierüber keine flächendeckende Cyberabwehrkompetenz des Bundes begründet werden kann.

IV. Besondere Abwehrmaßnahmen gemäß § 41a BPolG-E und §§ 68d, 68e BKAG-E – „Aktive Cyberabwehr“ („Hackback“)

1. Grundsatz und Risikoprofil aktiver Abwehrmaßnahmen (§ 41a Abs. 1 S. 1 Nr. 3 BPolG-E, § 68d BKAG-E)

Mit **§ 41a Abs. 1 Satz 1 Nr. 3 BPolG-E** und **§ 68d BKAG-E** stattet der Entwurf die Bundespolizei und das Bundeskriminalamt mit Befugnissen zur **aktiven Cyberabwehr** (umgangssprachlich: „**Hackback**“) aus.¹⁴ Angesichts der dramatisch verschärften Bedrohungslage – insbesondere durch staatlich gelenkte APT-Gruppen und professionalisierte Cybercrime-Netzwerke – ist der gesetzgeberische Wunsch verständlich, den Sicherheitsbehörden nicht nur rein passive Schutzschilde, sondern handlungsfähige operative Werkzeuge an die Hand zu geben. Dass bestimmte Angriffe nur durch aktive Maßnahmen wirksam abgewehrt werden können, spricht grundsätzlich für eine solche Befugnis; auch die grundrechtlichen Schutzpflichten sind hierbei zu berücksichtigen.¹⁵

¹³ BT-Drs. 21/6585, S. 64.

¹⁴ Zu Begriff und Einordnung des „Hackback“ *Barczak*, NJW 2020, 595 (596); *Martini/Klein*, Int. Cybersec. L. R. 2025, 63 (67).

¹⁵ Aus Perspektive der grundrechtlichen Schutzpflichten *Barczak*, NJW 2020, 595 (596); Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Impulspapier Aktive Cyberabwehr (2023), S. 5, <https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/publikationen/impulspapier-aktive-cyberabwehr> (zuletzt abgerufen am 04.10.2026).

Allerdings birgt der Schritt von der passiven Abwehr (wie dem Umleiten von Datenverkehr beim BSI) zum **aktiven, manipulierenden Zugriff auf fremde IT-Infrastrukturen** gravierende Risiken. Für die parlamentarische Beratung sind folgende Dimensionen entscheidend:

- **Das Dilemma der Kollateralschäden**

Cyberangreifer nutzen häufig fremde Rechner für ihre Angriffe. Sie kapern und verketteten weltweit fremde Server, Cloud-Instanzen oder Rechenzentren und schalten diese als „digitale Waffe“ vor. Wenn deutsche Behörden aktiv in ein solches Angriffssystem einwirken (z. B. durch Stilllegung oder Datenlöschung), können sie deshalb **Infrastrukturen unbeteiligter Dritter oder früherer Opfer** treffen.¹⁶ Wird hierbei etwa das kompromittierte Rechenzentrum eines Krankenhauses, eines Energieversorgers oder eines Telekommunikationsknotens versehentlich lahmgelegt, drohen verheerende physische und versorgungsrelevante Schäden.¹⁷

- **Völkerrechtliche Schranken**

Ein deutsches Gesetz kann Eingriffe auf ausländischem Hoheitsgebiet nicht schon für sich genommen völkerrechtlich legitimieren. Soweit Zielsysteme im Ausland stehen, muss die territoriale Souveränität des Sitzstaates gewahrt werden. Ein unautorisierter Zugriff kann sie insbesondere dann verletzen, wenn er physische Schäden oder erhebliche Funktionsbeeinträchtigungen verursacht. Eine innerstaatliche Befugnis ersetzt keine völkerrechtliche Grundlage; in Betracht kommen insbesondere die Zustimmung des Sitzstaates oder eng begrenzte völkerrechtliche Rechtfertigungsgründe, deren Voraussetzungen im Einzelfall nachzuweisen sind.¹⁸ Auch die Grundrechtsbindung deutscher Staatsgewalt endet nicht an der Staatsgrenze. Die völkerrechtliche Zulässigkeit und die grundrechtliche Rechtfertigung sind deshalb jeweils eigenständig zu prüfen.¹⁹

- **Erfordernis einer expliziten *Ultima-Ratio*-Klausel und Folgenprüfung**

Die Maßnahmen unterliegen bereits dem allgemeinen Verhältnismäßigkeitsgrundsatz (§ 16 BPolG, für das BKA über § 68a Abs. 3 BKAG-E). Hinzu kommen die

¹⁶ Bäcker/Golla, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 18 Rn. 25.

¹⁷ Martini/Klein, Int. Cybersec. L. R. 2025, 63 (91); Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Impulspapier Aktive Cyberabwehr (2023), S. 6; Barczak, NJW 2020, 595 (596).

¹⁸ Zu den völkerrechtlichen Grenzen Lui, TLJ 2024, 9 (11 ff.); Tallinn Manual 2.0, Rule 4, Rn. 4–5; Barczak, NJW 2020, 595 (597 ff.).

¹⁹ BVerfGE 154, 152 (BND Ausland-Ausland-Fernmeldeaufklärung); zu grundgesetzlichen Vorgaben für Hackbacks im Ausland Wissenschaftliche Dienste des Deutschen Bundestages, Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland, WD 3 – 3000 – 159/18, <https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf>.

technischen Schadensminderungsgebote des § 41a Abs. 4 BPolG-E und des § 68d Abs. 3 BKAG-E. Dies reicht angesichts der spezifischen Risiken jedoch nicht aus. Der Gesetzgeber sollte in den Normen ausdrücklich auch verankern:

- eine **strikte Subsidiarität (Ultima Ratio)**: Der aktive Eingriff darf erst erfolgen, wenn mildere defensive Schutzmaßnahmen (wie Netzsperrungen, Filterung oder DNS-Sinkholing im Rahmen der §§ 16, 16a BSI-G) ausgeschöpft sind oder offensichtlich keinen gleich wirksamen Schutz versprechen;
- eine **dokumentierte technische Risikofolgenabschätzung**, in der das Risiko von Kollateralschäden für unbeteiligte Systeme vorab zwingend dem erwarteten Abwehrerfolg gegenüberzustellen und die Auswahl der Maßnahme nachvollziehbar zu begründen ist.²⁰

Darüber hinaus ist zu prüfen, ob für besonders eingriffsintensive Maßnahmen eine **höhere Gefahrenschwelle** als die allgemeine Gefahr für die Sicherheit in der Informationstechnik erforderlich ist. Je größer das Schadenspotenzial des Eingriffs, desto gewichtiger müssen das bedrohte Rechtsgut und die abzuwehrende Gefahr sein.

2. Das staatliche Schwachstellen-Dilemma

Ein weitgehend ungelöstes Problem des Gesetzentwurfs ist die Frage, wie die Behörden technisch in die fremden Systeme eindringen sollen. Nach der Entwurfsbegründung soll dies auch durch das **Ausnutzen von IT-Sicherheitslücken** geschehen.²¹ Hierin liegt ein struktureller Widerspruch:

- Besonders problematisch ist die Nutzung von Sicherheitslücken, die dem Hersteller noch unbekannt sind (Zero-Day-Schwachstellen). Das operative Interesse an einem späteren Zugriff kann den Staat dazu verleiten, solche Lücken geheim zu halten, einzukaufen oder zu bevorraten, anstatt ihre Schließung anzustoßen.
- Solange eine Sicherheitslücke offen und ungepatcht bleibt, gefährdet sie gleichzeitig die IT-Sicherheit aller Bürger, Unternehmen und Behörden, die die betroffene Software einsetzen: Dieselbe Lücke kann auch von feindlichen Nachrichtendiensten oder Kriminellen ausgenutzt werden. Eine Maßnahme zur Stärkung der

²⁰ Aus Perspektive des internationalen Menschenrechtsschutzes *Martini/Klein*, Int. Cybersec. L. R. 2025, 63 (92); zur Verhältnismäßigkeit im konkreten Fall *Amthor*, GSZ 2020, 251 (256).

²¹ BT-Drs. 21/6585, S. 46.

Cybersicherheit kann auf diese Weise zugleich die Sicherheit anderer Systeme schwächen.²²

Das Bundesverfassungsgericht hat bereits 2021 hervorgehoben, dass den Staat eine **konkrete grundrechtliche Schutzpflicht** trifft, wenn Behörden eine Sicherheitslücke kennen, die dem Hersteller noch unbekannt ist. Gefordert ist eine grundrechtskonforme Regelung zur Auflösung des Zielkonflikts zwischen dem Schutz der Nutzer vor Angriffen Dritter und dem operativen Interesse an der Offenhaltung der Lücke. Daraus folgt allerdings keine Pflicht, jede Lücke sofort und unbedingt dem Hersteller zu melden. Eine konkrete Schutzpflichtverletzung hat das Gericht damals nicht festgestellt; die Verfassungsbeschwerde war unzulässig.²³

3. Empfehlung an den Gesetzgeber:

Das Gesetz darf den Sicherheitsbehörden keinen Blankoscheck zur unbefristeten Bevorratung von Sicherheitslücken ausstellen. Erforderlich ist ein **gesetzlich normiertes Schwachstellen-Management** (Vulnerabilities Equities Process): Erlangt eine Sicherheitsbehörde Kenntnis von einer gravierenden Zero-Day-Lücke, muss gesetzlich geregelt sein, nach welchen Kriterien, durch welches unabhängige Gremium und innerhalb welcher Höchstfristen entschieden wird, wann das operative Zugriffsinteresse hinter der Pflicht zur Benachrichtigung des Herstellers zum Schutze der Allgemeinheit zurückzutreten hat. Bis zu einer solchen gesetzlichen Einhegung sollte der Zugriff primär auf anderweitig rechtmäßig erlangte Zugangsdaten (Credentials) beschränkt werden.²⁴

4. Zurechnung und unvermeidbare Betroffenheit Dritter (§ 41a Abs. 3 BPolG-E, § 68d Abs. 4 BKAG-E)

Die Eingriffsbefugnisse sind auf Systeme begrenzt, von denen eine Gefahr ausgeht. Zu den „gefährgegenständlichen Daten“ zählen nach § 41a Abs. 2 BPolG-E und § 68d Abs. 2 BKAG-E neben Schadsoftware und Steuerungsdaten auch durch den Angriff entwendete oder weitergeleitete Daten. Erfasst werden damit sowohl Angreifer- als auch kompromittierte Opfersysteme, sofern von ihnen die maßgebliche Gefahr ausgeht.²⁵

Gemäß § 68d Abs. 4 BKAG-E und § 41a Abs. 3 BPolG-E dürfen Maßnahmen auch dann durchgeführt werden, wenn Dritte „**unvermeidbar betroffen**“ sind.

²² BVerfGE 158, 170 Rn. 36 ff., 39 ff. (IT-Sicherheitslücken); *Deusch/Eggendorfer*, K&R 2022, 797 (798); *Martini/Klein*, Int. Cybersec. L. R. 2025, 63 (91); Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Impulspapier Aktive Cyberabwehr (2023), S. 4.

²³ BVerfGE 158, 170, Leitsatz 2b, Rn. 20, 26, 34, 43–44 (IT-Sicherheitslücken).

²⁴ Diese Alternative nennt auch die Entwurfsbegründung, BT-Drs. 21/6585, S. 46.

²⁵ § 41a Abs. 1 Satz 1 Nr. 3, Abs. 2 BPolG-E; § 68d Abs. 1, 2 BKAG-E; zur Einbeziehung von Angreifer- und Opfersystemen BT-Drs. 21/6585, S. 45 f., 65 f.

Dies öffnet ein gefährliches Einfallstor für Fehleingriffe:

- Die technische Lokalisierung eines gefahrverursachenden Systems und die **Attribution** des Angriffs zu einer verantwortlichen Person oder Organisation sind auseinanderzuhalten. Selbst wenn sich ein Ausgangssystem hinreichend sicher bestimmen lässt, kann die Identität des Angreifers ungeklärt bleiben. Die Nutzung kompromittierter fremder Server, von Anonymisierungsdiensten und verschleierten Routing-Ketten erschwert diese Zurechnung zusätzlich.²⁶
- Die gesetzliche Klausel der „unvermeidbaren Betroffenheit“ darf nicht dazu führen, dass Behörden bei **vager oder unsicherer Faktenlage** auf Verdacht in Systeme eingreifen, deren funktionale Beteiligung an der Gefahr nicht hinreichend sicher festgestellt ist. Unsicherheit über die Identität des Angreifers und Unsicherheit über das gefahrverursachende System dürfen nicht gleichgesetzt werden.

5. Klarstellungsbedarf

Der Gesetzgeber sollte im Tatbestand unmissverständlich klarstellen: Die „unvermeidbare Betroffenheit Dritter“ meint ausschließlich unvermeidliche **technische Begleitfolgen am verifizierten Zielsystem** (z. B. minimale Beeinträchtigung anderer Nutzer auf demselben Großserver). Sie ermächtigt hingegen nicht zum Zugriff auf Systeme, bei denen schon die funktionale Beteiligung an der Gefahr nicht hinreichend sicher festgestellt und belastbar dokumentiert ist. Auch bei einem verifizierten System bleiben die Belange betroffener Dritter in die Verhältnismäßigkeits- und Folgenprüfung einzubeziehen.

6. Grundrechtliche Einordnung und Schutzniveau: Die verfehlte Differenzierung nach „privaten Systemen“ (§ 41a Abs. 1 S. 2, Abs. 5–8 BPolG-E, § 68e BKAG-E)

Der Entwurf unterwirft Zugriffe ohne Einwilligung des Betroffenen, die eine Datenerhebung ermöglichen, nur dann strengeren Anforderungen (qualifizierter Eingriffsanlass, Richtervorbehalt), wenn es sich um „**privat genutzte**“ Systeme handelt (§ 41a Abs. 1 Satz 2, Abs. 5–8 BPolG-E; § 68e BKAG-E).²⁷ Entscheidend ist bereits die Möglichkeit einer Datenerhebung, nicht erst eine tatsächliche Erhebung. Die Legaldefinition knüpft an die private Eigennutzung und die technische Möglichkeit eines aussagekräftigen Einblicks in die Lebensgestaltung oder Persönlichkeit an. Gemischte Nutzung ist damit nicht generell

²⁶ Schmoldt, ZFAS 2024, 165 (176 f.); Deusch/Eggendorfer, K&R 2022, 797 (798 f.); Lin, Journal of National Security Law & Policy 2010, 63 (77); Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Impulspapier Aktive Cyberabwehr (2023), S. 2.

²⁷ Zum Eingriffsanlass § 41a Abs. 5 BPolG-E bzw. § 68e Abs. 1 BKAG-E; zum Richtervorbehalt § 41a Abs. 6 BPolG-E bzw. § 68e Abs. 3, 4 BKAG-E.

ausgeschlossen. Nach der Begründung sollen jedoch ausschließlich für Angriffe betriebene Systeme und Systeme mit lediglich unbedeutender privater Mitnutzung nicht erfasst sein.²⁸ Die Verknüpfung des erhöhten Schutzes mit dem zusätzlichen Merkmal „privat“ bleibt problematisch.

Diese Konstruktion verkennt die Schutzrichtung des **Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)**. Die nachfolgend herangezogenen Entscheidungen betreffen andere staatliche Zugriffe auf IT-Systeme, insbesondere Überwachungsmaßnahmen. Die dort entwickelten Maßstäbe sind auf die hier geregelten Abwehrmaßnahmen unter Berücksichtigung ihres jeweiligen Zwecks und ihrer Eingriffswirkung zu übertragen:

a) Schutzbereich erfasst auch geschäftliche und gemischte Nutzung

Nach ständiger Karlsruher Rechtsprechung schützt das IT-System-Grundrecht Systeme, die allein oder durch ihre Vernetzung personenbezogene Daten enthalten können, die Rückschlüsse auf wesentliche Teile der Lebensgestaltung oder ein aussagekräftiges Bild der Persönlichkeit zulassen.²⁹ Dieser Schutz ist **ausdrücklich nicht auf den häuslich-privaten Bereich beschränkt**.³⁰ Auch geschäftlich genutzte Laptops, Smartphones oder Unternehmensserver können höchst persönliche Korrespondenzen, Bewegungsdaten und Kommunikationsprofile enthalten. Geschützt wird zudem nicht nur die Vertraulichkeit vorhandener Daten, sondern auch die Integrität des Systems: Schon dessen technische Infiltration kann persönlichkeitsrelevante Erhebungen ermöglichen und entsprechende Risiken begründen.³¹

b) Kriterium der Eigennutzung statt pauschalem Ausschluss

Zwar können reine Steuerungsrechner (wie isolierte C2-Server), die keinen hinreichenden Personenbezug aufweisen, bereits tatbestandlich aus dem IT-System-Grundrecht herausfallen. Sobald ein System jedoch von einer natürlichen Person als eigenes genutzt wird und nach seiner technischen Funktionalität oder Vernetzung einen aussagekräftigen Einblick in ihre Lebensgestaltung oder Persönlichkeit ermöglichen kann, greift der Grundrechtsschutz – unabhängig davon, ob die Nutzung privater oder beruflicher Natur ist. Auch die Nutzung eines solchen Systems für rechtswidrige Angriffe beseitigt den

²⁸ § 41a Abs. 5 Satz 2 BPolG-E; § 68e Abs. 2 BKAG-E; BT-Drs. 21/6585, S. 48, 67.

²⁹ BVerfGE 120, 274 (308); BVerfGE 172, 46 Rn. 97 ff.

³⁰ BVerfGE 120, 274 (314); *Eichberger*, in: Huber/Voßkuhle, 8. Aufl. 2024, Art. 2 GG Rn. 345, auch zum Schutz geschäftlicher Daten; zum möglichen Vorliegen personenbezogener Daten als Schutzbereichsvoraussetzung *Heckmann/Paschke*, in: Stern/Sodan/Möstl, StaatsR IV, 2. Aufl. 2022, § 103 Rn. 18.

³¹ BVerfGE 172, 46 Rn. 99–100; BVerfGE 120, 274 (308); *Rixen*, in: Sachs, 10. Aufl. 2024, Art. 2 GG Rn. 73d; zur dogmatischen Einordnung kritisch *Eifert*, NVwZ 2008, 521 (522).

Schutzbereich nicht. Nicht jede geringfügige Mitnutzung erfüllt allerdings schon die genannten Schutzbereichsvoraussetzungen.³²

c) Opfersysteme als typischer Anwendungsfall

Da aktive Abwehrmaßnahmen auch gegen **missbrauchte Opfersysteme** (z. B. kompromittierte Unternehmensserver oder vernetzte Endgeräte unbeteiligter Bürger) gerichtet werden können, drohen hier schwerwiegende Grundrechtseingriffe. Das gilt auch für Eingriffe, die Schadsoftware beseitigen oder Sicherheitslücken schließen sollen. Dass der Inhaber des Geräts Opfer eines Angriffs geworden ist, mindert seinen Grundrechtsschutz nicht.

Hinzu kommt ein praktisches **Abgrenzungsproblem**: Die Behörde müsste bereits vor dem Zugriff wissen, ob und in welchem Umfang ein System privat, beruflich oder für Angriffe genutzt wird. Gerade hierzu kann ihr aber die erforderliche Kenntnis der Systeminhalte fehlen. Die Begründung stellt bei „unbedeutender“ privater Mitnutzung auf Umfang und Vielfalt der Daten ab; diese Bewertung darf nicht erst durch denjenigen Zugriff gewonnen werden, dessen Schutzanforderungen sie bestimmen soll.³³

7. Empfehlung

Die starre und in der Praxis kaum handhabbare Unterscheidung zwischen „privaten“ und „nicht-privaten“ Systemen sollte aufgegeben werden. Der Richtervorbehalt und die qualifizierten Verfahrenssicherungen müssen **für jeden verdeckten, manipulierenden oder datenerhebenden Zugriff auf eigengenutzte IT-Systeme** gelten, der die genannten Schutzbereichsvoraussetzungen erfüllt und ohne wirksame Einwilligung erfolgt – insbesondere dann, wenn auf Opfersysteme eingewirkt wird. Eine Differenzierung zwischen Angreifern und Opfern gehört nicht in die künstliche Verengung des Grundrechtstatbestands, sondern hat ihren dogmatisch richtigen Platz allein auf der **Ebene der verfassungsrechtlichen Rechtfertigung (Verhältnismäßigkeit)**. Dort können abgestufte Eingriffsschwellen erwogen werden; ihre Anwendung setzt jedoch eine belastbare Zuordnung der jeweiligen Rolle voraus.³⁴

³² Vgl. BVerfGE 172, 106 Rn. 173, 175 zu den Schutzbereichsvoraussetzungen; zur Einbeziehung von Angriffssystemen *Ziegler/Kemper*, Das BKA als Cyberabwehrbehörde, VerBlog v. 24.3.2026, <https://verfassungsblog.de/das-bka-als-cyberabwehrbehorde/>.

³³ BT-Drs. 21/6585, S. 48, 67. Die Entwurfsbegründung versteht private Mitnutzungen als unbedeutend, wenn Umfang oder Vielfalt der Daten keinen Einblick in wesentliche Teile der Lebensgestaltung und kein aussagekräftiges Persönlichkeitsbild ermöglichen.

³⁴ Zur Verortung einer Differenzierung auf der Rechtfertigungsebene *Ziegler/Kemper*, Das BKA als Cyberabwehrbehörde, VerBlog v. 24.3.2026, <https://verfassungsblog.de/das-bka-als-cyberabwehrbehorde/>.