



Ausschussdrucksache 21(4)221 A
vom 30. September 2026

Schriftliche Stellungnahme

von Dr. Sven Herpig, Leiter Cybersicherheit und Neue Bedrohungen
bei Interface vom 28.09.2026

zu dem

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

interface I

Stellungnahme von Dr. Sven Herpig, Lead Cybersecurity & Emerging Threats bei interface – Tech analysis and policy ideas for Europe e.V. (ehemals: Stiftung Neue Verantwortung), für die Öffentliche Anhörung des Innenausschusses des Deutschen Bundestags am 5. Oktober 2026 zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (BT-Drucksache 21/6585).

Kontakt

[Dr. Sven Herpig](#)

Lead Cybersecurity & Emerging Threats

[interface – Tech analysis and policy ideas for Europe e.V.](#)

Email: sherpig@interface-eu.org

Github: <https://github.com/z-edian/publications>

interface I

Zusammenfassung

Der Gesetzentwurf erweitert intrusive Cyberabwehrbefugnisse erheblich. Gegenüber dem Referentenentwurf vom Februar 2026 greift der Gesetzentwurf einzelne Kritikpunkte und Empfehlungen aus meiner damaligen Stellungnahme auf: Die Eingriffsbefugnisse sind auf gefahrgegenständliche Daten und auf Systeme beschränkt, von denen die Gefahr ausgeht, es gilt ein Straftatenkatalog, und Kontrollmechanismen wurden ergänzt – Pflichtkontrollen durch die BfDI, Benachrichtigungspflichten sowie für die Bundespolizei eine Berichtspflicht gegenüber dem Bundestag. Gleichzeitig kommen neue Befugnisse hinzu, insbesondere Übermittlungspflichten an die Bundeswehr sowie erweiterte Anordnungsbefugnisse gegenüber Telekommunikations- und Digitale-Dienste-Anbietern. Zentrale strukturelle Probleme bleiben jedoch ungelöst:

- Fragmentierte Zuständigkeiten,
- Inkohärente Eingriffsschwellen,
- Fehlende Governance für intrusive Werkzeuge,
- Unzureichende Stärkung von Resilienz.

Ohne Koordinationsmechanismen und Transparenzstandards drohen Effektivitätsverluste und rechtliche Unsicherheiten.

interface I

1. Vorbemerkung

Der vorliegende Gesetzentwurf¹ behandelt das Thema „Cyberabwehr“, auch bekannt als „Aktive Cyberabwehr“, „Gefahrenabwehr im Cyberraum“ oder „Hackback“. interface versteht unter diesem Begriff Maßnahmen, bei denen ein einzelner oder mehrere Staaten gemeinsam (intrusive) technische Eingriffe anordnen oder durchführen lassen, um eine aktuelle, spezifische Cyberoperation oder -kampagne zu neutralisieren, zu mitigieren oder zuzuordnen.² Die im Gesetzentwurf genannten Instrumente, etwa in BKAG-E § 68d, richten sich gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme zur proaktiven Abwehr maliziöser Cyberaktivitäten, einschließlich der Systeme unvermeidbar betroffener Dritter gemäß BKAG-E § 68d (4), und fallen damit unter diese Definition.

Der politische und fachliche Diskurs über diese Form der Cyberabwehr zieht sich seit fast zehn Jahren hin³, ohne nennenswerte Fortschritte – abgesehen von BSIG §§ 16 und 17. Ursachen dafür sind sowohl oberflächlich geführte Debatten als auch bewusste Nebelkerzen, wie die Umdeutung des Begriffs „Hackback“.⁴ Auch frühere Initiativen – etwa der Vorstoß des Präsidenten des Bundespolizeipräsidiums, Dr. Dieter Romann, im Rahmen der Neustrukturierung des Bundespolizeigesetzes 2024⁵ scheiterten. Parallel zu den vom Bundesministerium des Innern (BMI) geplanten Ausweitungen intrusiver Cyberabwehrbefugnisse für Bundeskriminalamt (BKA) und Bundespolizei (BPol) sollen auch beim Bundesnachrichtendienst (BND) und beim Bundesamt für Verfassungsschutz (BfV) intrusive Cyberbefugnisse geschaffen bzw. erweitert werden.⁶

Bevor die Befugnisse für aktive Cyberabwehr erweitert werden, muss zunächst klar benannt werden, welche Risiken damit verbunden sind. Unbeabsichtigte Kollateralschäden sowie die mögliche Proliferation der eingesetzten Werkzeuge können die Lage schnell verschärfen. Fehlzuordnungen könnten zudem dazu führen, dass Maßnahmen gegen kompromittierte Drittinfrastruktur oder unbeteiligte Betreiber gerichtet werden – mit dem Risiko diplomatischer oder rechtlicher Konflikte in Drittstaaten. Auch die Frage, wer für Schäden bei Dritten haftet, die durch angeordnete Maßnahmen entstehen, bleibt offen: Die Bundesregierung verneint Haftungsansprüche gegenüber mitwirkenden Unternehmen lediglich „grundsätzlich“, eine

¹ [Deutscher Bundestag \(2026\): Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Stärkung der Cybersicherheit](#)

² [Sven Herpig \(2023\): Active Cyber Defense – Toward Operational Norms](#)

³ [Sven Herpig et al. \(2020\): Aktive Cyberabwehr/ Hackback in Deutschland](#)

⁴ [Sven Herpig \(2022\): Aktive Cyberabwehr statt Hackback?](#)

⁵ [Dieter Romann \(2024\): Schriftliche Stellungnahme des Präsidenten des Bundespolizeipräsidiums Herrn Dr. Dieter Romann zur öffentlichen Anhörung am 22. April 2024 zum Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes BT-Drucksache 20/10406](#)

⁶ [Bundesministerium des Innern \(2026\): Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts, 05.07.2026](#)

interface I

gesetzliche Klarstellung sieht der Entwurf nicht vor.⁷ Unter sorgfältiger Auswahl und Abwägung sowie mit robusten Schutzmechanismen können solche Maßnahmen die nationale Cybersicherheit zwar erhöhen. Entscheidend ist jedoch, dass sie konsequent in bestehende Sicherheitskultur, IT-Architektur und strategische Konzepte eingebettet werden. Ohne diese Einbettung droht ein Ungleichgewicht zwischen operativer Handlungsmacht und tatsächlicher Sicherheitswirkung – ein Problem, das bereits in vergleichbaren Diskussionen um hochinvasive Cyberbefugnisse deutlich wurde.

Offene, differenzierte technische und politische Debatten über Anwendungsfälle, Kriterien und Schutzvorkehrungen sind dabei unerlässlich. Nur so wird das Verursachen von Kosten für Angreifende nicht zur bloßen symbolischen Demonstration staatlicher Handlungsfähigkeit. In der Praxis werden aktive Cyberabwehrmaßnahmen ohnehin nur einen kleinen Teil des Portfolios ausmachen, das die Cybersicherheit stärkt; IT-Sicherheit und Resilienz bleiben die zentralen Säulen der nationalen Sicherheit im Cyberraum.⁸ Dies wird u. a. am Beispiel des jüngsten IT-Sicherheitsvorfalls bei der Berliner Senatsverwaltung deutlich⁹: Keine der im vorliegenden Gesetzentwurf geforderten intrusiven Befugnisse hätte den Vorfall abwenden oder den Schaden mitigieren können.

Vor diesem Hintergrund sollte die Bundesregierung intrusive Maßnahmen auf das notwendige Minimum beschränken und sich auf nicht-intrusive, bedrohungsunabhängige, skalierbare und nachhaltige Schritte zum Schutz der eigenen IT-Infrastruktur konzentrieren. Reicht dies in Einzelfällen nicht aus, erfordert eine verantwortungsvolle Durchführung die Wahl der am wenigsten intrusiven und eskalierenden Gegenmaßnahmen (z. B. „Walled-Garden-Anordnung“ statt begrenzter „Eingriffe in informationstechnische Systeme von Geschädigten („Opfersysteme“), von denen im Rahmen eines Cyberangriffs eine Gefahr ausgeht“). Diese müssen effizient, wirksam und verhältnismäßig sein. Zugleich gilt: Der wirtschaftliche, politische, sicherheits- und gesellschaftliche Schaden des Nicht-Handelns muss größer sein als die Kosten, die eine aktive Cyberabwehr verursacht.¹⁰

⁷ [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

⁸ [Sven Herpig \(2021\): Active Cyber Defense Operations – Assessment and Safeguards](#)

⁹ [Sven Herpig, Alexandra Paulus und Johannes Steger \(2026\): CN016 Sonderfolge: Einbruch in die Berliner Senatsverwaltung](#)

¹⁰ [Sven Herpig \(2023\): Active Cyber Defense – Toward Operational Norms](#)

2. Kritik

2.1 Parallelstrukturen gefährden Effektivität

Wie bereits in der Vorbemerkung hervorgehoben, ist die bestehende Sicherheitsarchitektur entscheidend für die Effektivität und Effizienz geplanter Cyberabwehrmaßnahmen. Der aktuelle Gesetzentwurf plant jedoch eine Ausweitung der Befugnisse, ohne die bekannten Defizite der deutschen Cybersicherheitsarchitektur zu adressieren.¹¹

Neben den bestehenden Befugnissen der Länderpolizeien im Bereich Gefahrenabwehr im Cyberraum sollen die Kompetenzen für BSI und für BfV und BND (parallel durch NDRRefG-E) erweitert, für das BKA deutlich ausgeweitet und für die Bundespolizei neu geschaffen werden. Der Entwurf sieht jedoch weder verbindliche Einvernehmensregelungen (lediglich Benehmensregelungen gemäß BPolG-E § 41a (10) und BKAG-E § 68c (3)) noch Konfliktlösungsmechanismen oder abgestimmte Koordinationsprozesse (lediglich Benachrichtigungen gemäß BKAG-E § 3a (4)) vor. Selbst wenn solche Mechanismen vorgesehen wären, fehlt bislang eine operative Plattform, auf der alle relevanten Behörden vertreten sind und sich koordinieren könnten. Ohne formalisierten Abstimmungsprozess könnten künftig alle genannten Behörden parallel aktive Cyberabwehrmaßnahmen durchführen – weitgehend unabhängig voneinander oder mit nur begrenzten Koordinationsmechanismen.

Erschwerend kommt hinzu, dass der Umgang des Staates mit Schwachstellen, die für bestimmte Cyberabwehroperationen, zum Beispiel gemäß BPolG-E § 41a (s. Begründung), erforderlich sein könnten, weiterhin ungeklärt bleibt. Deutschland verfügt bislang über kein transparentes Verfahren zur staatlichen Entscheidung über das Zurückhalten oder Offenlegen von Schwachstellen.¹² Risiken und rechtliche Grauzonen bestehen daher fort.¹³ Die geplante Parallelstruktur einer aktiven Cyberabwehr durch BKA, BSI, Bundespolizei und die Länder – neben ähnlich gelagerten Zuständigkeiten bei BfV, BND und Bundeswehr – schafft mehrere operative Säulen ohne klare Priorisierung oder Abstimmungsregeln mit dem BSI als zentraler

¹¹ [Sven Herpig \(2023\): Stellungnahme von Dr. Sven Herpig, Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. \(SNV\), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland"](#) und [Bundesrechnungshof \(2025\): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit](#)

¹² [Gesellschaft für Freiheitsrechte \(2026\): Rechtsgutachten: Staatlicher Umgang mit IT-Schwachstellen und Spyware - Verfassungsrechtliche Anforderungen und Grenzen](#) und [Sven Herpig \(2018\): Schwachstellen-Management für mehr Sicherheit – Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte](#)

¹³ [Sven Herpig \(2023\): Stellungnahme von Dr. Sven Herpig, Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. \(SNV\), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland"](#) und [Sven Herpig \(2025\): Schriftliche Stellungnahme von Dr. Sven Herpig, interface vom 8. Oktober 2025 – Öffentliche Anhörung – Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung BT-Drucksache 21/1501](#)

interface I

Cybersicherheitsbehörde des Bundes. Die Bundesregierung stellt zudem klar, dass Übermittlungen des BSI nach BSIG-E § 8 (6) und (7) auch künftig nicht auf die Strafverfolgung begrenzt sind, sondern ebenso Zwecke der Gefahrenabwehr und „Gefahrenaufklärung“ umfassen.¹⁴ Neu hinzu kommt die Übermittlung an die Bundeswehr (BSIG-E § 8 (6) Satz 2 Nummer 4), die der Entwurf auch für BKA und BPol vorsieht (BKAG-E § 68a (4), BPolG-E § 41a (13)). Daten fließen damit an noch mehr operative Säulen, ohne dass geregelt ist, wer auf ihrer Grundlage handelt.

Das erinnert an ein ähnliches Vorgehen bei den Sicherheitsgesetzen Ende 2019. Damals resümierten Dr. Ulf Buermeyer und ich: „Statt weiteren Behörden weitreichende Befugnisse einzuräumen, müsste die Lösung eher darin bestehen, Zuständigkeiten klarer zu definieren und das bisherige Nebeneinander und oftmals auch Gegeneinander von Sicherheitsbehörden zu beenden. Stattdessen wird der Ausbau der Sicherheitsgesetzgebung mit teils massiven Eingriffen in die Grundrechte der Bürgerinnen und Bürger weiter vorangetrieben [...]“.¹⁵

Das geplante Vorgehen droht, Ressourcen zu zersplittern, Verantwortlichkeiten zu verwässern und die Gesamteffektivität der Cyberabwehr für die nationale Sicherheit zu mindern.

2.2 Befugnisse statt Resilienz

Wie in der Vorbemerkung betont, sind offene und differenzierte technische sowie politische Debatten über Anwendungsfälle, Kriterien und Schutzvorkehrungen unerlässlich. Nur so wird das Verursachen von Kosten für Angreifende nicht zu einer bloßen symbolischen Demonstration staatlicher Handlungsfähigkeit. In der Praxis werden aktive Cyberabwehrmaßnahmen ohnehin nur einen kleinen Teil der Maßnahmen ausmachen, die die Cybersicherheit insgesamt stärken; IT-Sicherheit und Resilienz bleiben die zentralen Säulen.

Diese Säulen werden unter anderem durch die erweiterten Befugnisse des BSI gestärkt. Gemäß BSIG-E § 11 (1) Satz 1 erhält das BSI die Befugnis, in herausgehobenen Fällen auf Ersuchen der betroffenen Einrichtung „zur Suche und Identifikation der Beeinträchtigung der Sicherheit oder Funktionsfähigkeit [der] informationstechnischen Systeme“ tätig zu werden. Von diesen sogenannten Threat-Hunting-Operationen¹⁶ soll das BSI auf Basis der im Gesetzentwurf vorgesehenen Personalstellen vorerst drei Aktivitäten pro Jahr durchführen können. Selbst wenn hierfür auch Personal aus der Vorfallsbearbeitung eingesetzt wird, ist dies zu wenig, um die Ausweitung der Befugnisse zu rechtfertigen. Der Gesetzentwurf sollte deutlich mehr Stellen

¹⁴ [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

¹⁵ [Ulf Buermeyer und Sven Herpig \(2019\): Immer neue Sicherheitsgesetze helfen nicht](#)

¹⁶ [Sven Herpig \(2022\): Cybersicherheitspolitik: Deutsche Ideenlosigkeit?](#)

interface I

für die Bereiche Vorfallsbearbeitung und Threat Hunting vorsehen, um die IT-Sicherheit und Resilienz substantiell zu stärken. Gleichzeitig sollte das BSI prüfen, seine operative Handlungsfähigkeit strategisch zu erweitern und interne Stellen gezielt in operative Arbeitsbereiche zu verschieben.

Vor dem Hintergrund der politischen Versprechen der Bundesregierung zu Bürokratieabbau und Ausgabendisziplin wirkt der im Gesetzentwurf vorgesehene Ausbau von rund 350 Stellen bis 2031 für teils hochinvasive und personalintensive aktive Cyberabwehrmaßnahmen bei BKA und BPol politisch und strategisch fragwürdig. Vor allem, weil unklar bleibt, welches konkrete Mehr an nachhaltiger Cybersicherheit hierdurch erzielt werden kann. Tom Uren, ehemaliger Mitarbeiter des australischen Verteidigungsministeriums schrieb hier vor Kurzem: "Even very effective takedowns and disruptive cyber operations are speed bumps rather than roadblocks. They slow adversaries, but don't stop them."¹⁷ Vor diesem Hintergrund steht der Ansatz des Gesetzentwurfes im Widerspruch zu den empirisch belegten Herausforderungen der IT-Infrastruktur in Deutschland: Die zentralen und dezentralen Systeme der Bundesverwaltung bezeichnete der Bundesrechnungshof im Sommer 2025 in seinem Prüfbericht als „unverändert defizitär“.¹⁸ Er empfahl, Standardmaßnahmen zur IT-Sicherheit und Resilienz zu stärken – über die Notwendigkeit aktiver Cyberabwehr verlor er kein Wort.

Die geplanten Ausweitungen aktiver Cyberabwehrbefugnisse sind angesichts begrenzter personeller Kapazitäten und fehlender Koordination unverhältnismäßig und adressieren nicht die eigentlichen Defizite in IT-Sicherheit und Resilienz. Effektiver Schutz erfordert stattdessen eine Stärkung standardisierter Sicherheitsmaßnahmen und operativ handlungsfähiger Strukturen bei den Betreibern der IT des Bundes und beim BSI.

2.3 Rechtsunsicherheit und Fragmentierung

Mit der Verortung vor allem intrusiver Cyberabwehrbefugnisse beim BKA ist in den vergangenen Jahren im politischen Prozess immer wieder eine zentrale Frage aufgetaucht: die verfassungsrechtliche Zuständigkeit. Die Gefahrenabwehr ist grundsätzlich Aufgabe der Länder, wobei der Bund nur unter bestimmten Voraussetzungen eigene Zuständigkeiten wahrnehmen kann. Vor diesem Hintergrund wurde mehrfach auf die Notwendigkeit einer Grundgesetzänderung hingewiesen, sollten dem BKA derartige Befugnisse übertragen werden.

Nach der Bundestagswahl 2025 war jedoch klar, dass die Bundesregierung die dafür erforderliche Zweidrittelmehrheit im Parlament nicht erreichen würde. Stattdessen verteilt die

¹⁷ [Tom Uren \(2026\): Srsly Risky Biz: Trump's Cyber Strategy... Great, Amazing, The Best Yet](#)

¹⁸ [Bundesrechnungshof \(2025\): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit](#)

interface I

Bundesregierung die Befugnisse auf BPol, BSI, BfV, BND und BKA. Die Anpassungen am BPolG, BSIg und BKAG erfolgen – ebenso wie die parallelen Vorhaben im Nachrichtendienstrecht – lediglich auf Ebene des einfachen Gesetzes. Diese „Strategie“ führt jedoch zu einer starken Zersplitterung der Zuständigkeiten, schafft Überschneidungen und erschwert eine kohärente und effiziente Cyberabwehr auf Bundesebene.

Die BKAG-E §§ 68b–68d eröffnen dem Bundeskriminalamt weitreichende Befugnisse: von der Untersagung des Betriebs informationstechnischer Systeme über die Umleitung und Unterbindung von Datenverkehr bis hin zu Eingriffen in Systeme durch Auslesen, Löschen oder Verändern gefahrgegenständlicher Daten – teilweise auch ohne Wissen der Betroffenen. Wie ein Auslesen, Löschen oder Verändern gefahrgegenständlicher Daten ohne weitere technische Veränderungen am betroffenen System funktionieren soll, bleibt offen. Der Entwurf setzt solche Veränderungen selbst voraus, denn BKAG-E § 68d (3) Satz 2 verpflichtet dazu, sie nach Beendigung der Maßnahme rückgängig zu machen. Die Maßnahmen sind zudem nicht als isolierte Ausnahmeinstrumente konzipiert, sondern systematisch in die allgemeine Gefahrenabwehr integriert und knüpfen zwar an einen Straftatenkatalog an (BKAG § 3a Absatz 2), im Übrigen aber an weit gefasste Aufgabenzuweisungen: Während BKAG-E § 3a (1) Nummer 1 schwerwiegende Gefahren voraussetzt, die nur gemeinsam mit öffentlichen Stellen anderer Staaten oder mit zwischen- und überstaatlichen Stellen abgewehrt werden können, genügt nach Nummer 2 jede Gefahr, die sich gegen die Funktionsfähigkeit von Behörden oder Einrichtungen des Bundes richtet – ohne Erheblichkeitsschwelle. Nummer 3 stellt zusätzlich auf Auswirkungen auf die Stellung in der Staatengemeinschaft oder die Verteidigung ab.

Auffällig ist zudem das Verhältnis der Eingriffsschwellen zwischen den Behörden. Das BSI darf Anbieter nur „zur Abwehr erheblicher Gefahren“ anweisen, Datenverkehr umzuleiten oder zu unterbinden, und auch nur, soweit dies technisch möglich und wirtschaftlich zumutbar ist (BSIG-E § 17 (2)). Dasselbe gilt für Anordnungen gegenüber Top Level Domain Name Registries (BSIG-E § 16a (1)). BKA und BPol können eine vergleichbare Anordnung gegenüber Telekommunikations- und Digitale-Dienste-Anbietern bereits treffen, wenn von dem Datenverkehr „eine Gefahr“ ausgeht (BKAG-E § 68c (2), BPolG-E § 41a (9)). Zwar muss es sich dabei um eine im Einzelfall bestehende Gefahr der Verwirklichung einer Katalogstraftat handeln (BKAG-E § 68a (2)), ein Erheblichkeitserfordernis folgt daraus aber nicht. Auch für das Auslesen, Löschen und Verändern von Daten, die eingriffsintensivste der vorgesehenen Maßnahmen, gilt außerhalb privater Systeme keine erhöhte Schwelle, erst dort sind „dringende Gefahren“ erforderlich (BKAG-E § 68e (1), BPolG-E § 41a (5)). Selbst die Übermittlung von Daten durch das BSI an die Polizeien des Bundes und der Länder zur Gefahrenabwehr setzt eine Gefahr für den Bestand oder die Sicherheit des Staates, für Leib, Leben oder Freiheit einer

interface I

Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist voraus und bedarf der vorherigen gerichtlichen Zustimmung (BSIG-E § 8 (7)). Die Behörde mit den am wenigsten intrusiven Befugnissen unterliegt damit den höchsten Eingriffsschwellen. Dieser Wertungswiderspruch lässt sich mit der unterschiedlichen Eingriffsintensität der Maßnahmen nicht begründen.

Der weit gezogene Anwendungsbereich spiegelt sich auch im Personalbedarf von 264 Stellen bis 2031 wider. Auch wenn für Eingriffe in private Systeme zusätzliche gerichtliche Hürden vorgesehen sind, wird der Anwendungsbereich strukturell weit gezogen. Eine Behandlung als bloße Detailkorrektur würde damit die qualitative Erweiterung staatlicher Eingriffsbefugnisse im digitalen Raum unterschätzen. Angesichts der Intensität der vorgesehenen Maßnahmen und ihrer potenziellen Reichweite drängt sich die Frage auf, ob hier nicht eine offene verfassungsrechtliche Grundsatzdebatte – einschließlich der Frage nach einer Grundgesetzänderung – geführt werden müsste, statt die Neuregelung als punktuelle Anpassung zu behandeln. Die Bundesregierung stützt die Unterscheidung zwischen privaten und nicht-privaten Systemen – und damit den auf private Systeme beschränkten Richtervorbehalt – auf die Beschlüsse des Bundesverfassungsgerichts vom 24. Juni 2025.¹⁹ Ob diese Differenzierung in der Praxis trägt, ist zweifelhaft, da informationstechnische Systeme häufig gemischt genutzt werden und die Abgrenzung oft erst im Nachhinein möglich ist.

Die geplante Verlagerung intrusiver Cyberabwehrbefugnisse zum BKA und die Ausweitung von Eingriffsmöglichkeiten ohne offene verfassungsrechtliche Debatte führen zu einer Zersplitterung der Zuständigkeiten und einer erheblichen Rechtsunsicherheit. Angesichts der Reichweite und Intensität der Maßnahmen ist eine grundsätzliche Diskussion über die verfassungsrechtliche Legitimation dringend geboten.

2.4 Unklare Transparenz und Governance

Wie bereits in der Vorbemerkung betont, sind transparente und wirksame Schutzvorkehrungen unverzichtbar, wenn Sicherheitsbehörden neue intrusive Befugnisse erhalten.²⁰ Der vorliegende Gesetzentwurf spezifiziert solche Schutzmechanismen bislang jedoch nur unvollständig. Vorgesehen sind die Kontrolle durch die BfDI (BPolG-E § 77, BKAG-E § 69), Benachrichtigungspflichten (BPolG-E § 78, BKAG-E § 74) und die Löschregelungen (BPolG-E § 81, BKAG-E § 79). Nicht geregelt sind dagegen Beschaffung und Verwaltung technischer Werkzeuge, die Dokumentation aller Maßnahmen und die Sicherung digitaler Beweismittel. Der

¹⁹ [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

²⁰ [Sven Herpig \(2018\): A Framework for Government Hacking in Criminal Investigations](#)

interface I

Bundesrat fordert aus diesem Grund, dass sämtliche Eingriffe nach BKAG-E § 68d (1) einer richterlichen Anordnung bedürfen, unabhängig von der Nutzungsart des betroffenen Systems. Die Bundesregierung lehnt dies ab.²¹ Hinzu kommt, dass der Entwurf für die vorgesehenen Richtervorbehalte nach BKAG-E § 68e (3) und § 68f (2) weder das zuständige Gericht noch die anzuwendende Verfahrensordnung bestimmt, anders als für die Bundespolizei in BPolG-E § 41a (6) und (11), sodass diese Schutzmechanismen derzeit ins Leere laufen. Die Bundesregierung hat eine Ergänzung von BKAG § 90 im parlamentarischen Verfahren angekündigt.²²

Unklar bleibt insbesondere, nach welchen Standards und aus welchen Quellen BKA und Bundespolizei Schwachstellen, Exploits oder andere technische Werkzeuge für intrusive Cyberabwehroperationen beschaffen und wie diese anschließend verwaltet werden sollen (geregelt ist lediglich deren Schutz gegen unbefugte Nutzung gemäß BPolG-E § 41a (4) Nummer 3 und BKAG-E § 68d (3) Satz 3). Angesichts der erheblichen Risiken und der problematischen Marktstruktur für solche Fähigkeiten wäre hier ein deutlich höheres Maß an Transparenz und Regulierung erforderlich.²³

Für die Bundespolizei unterwirft der Entwurf die Maßnahmen nach BPolG-E § 41a (1) Satz 1 Nummer 2 und 3 immerhin der Berichtspflicht gegenüber dem Deutschen Bundestag (BPolG-E § 106). Für das BKA fehlt eine entsprechende Regelung: BKAG § 88 bleibt unverändert, obwohl dort ebenfalls die intrusivsten Befugnisse verortet werden. Ein Berichtssystem analog zu den Statistiken des Bundesamts für Justiz zur Telekommunikationsüberwachung könnte hier Abhilfe schaffen.²⁴ Insbesondere für Eingriffe nach BPolG-E § 41a (1) Satz 1 Nummer 3 und BKAG-E § 68d wäre eine solche Dokumentation notwendig, um Anwendungshäufigkeit, Effektivität und Verhältnismäßigkeit im Nachhinein beurteilen zu können. Eine statistische Erfassung wird lediglich in der Gesetzesbegründung erwähnt. Im Normtext fehlt sie.

Schließlich ist bei polizeilichen Maßnahmen die Integrität der Beweismittelkette von zentraler Bedeutung – auch im digitalen Raum. Gerade vor dem Hintergrund erweiterter Befugnisse zum Löschen oder Verändern von Daten, etwa gemäß BKAG-E § 68d, wären klare technische Standards und Governance-Mechanismen erforderlich, um die Nachvollziehbarkeit und gerichtliche Verwertbarkeit digitaler Beweise sicherzustellen. Der Entwurf erstreckt die Protokollierungspflicht nach BKAG § 82 auf Maßnahmen nach BKAG-E § 68d nur in Verbindung

²¹ [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

²² [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

²³ [Foreign, Commonwealth & Development Office \(2025\): The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities](#) und [Sven Herpig \(2018\): A Framework for Government Hacking in Criminal Investigations](#)

²⁴ [Bundesamt für Justiz \(2025\): Statistiken zur Telekommunikationsüberwachung für das Jahr 2023 veröffentlicht](#)

interface I

mit § 68e, also ausschließlich auf Eingriffe in private Systeme, ergänzt um Angaben zur Identifizierung des betroffenen Systems. Für alle übrigen Eingriffe des BKA – einschließlich des Löschens und Veränderns von Daten in Unternehmens- und Opfersystemen – fehlen Protokollierungs- und Dokumentationspflichten im Normtext. Für die Bundespolizei gilt die entsprechende Pflicht dagegen für alle Maßnahmen nach BPolG-E § 41a (1) Satz 1 Nummer 3 (BPolG-E § 85). Ähnliches gilt für die Übermittlung sicherheitsrelevanter Informationen an das BSI nach BSIG-E § 15 (6): Gesetzliche Anforderungen an die Sicherheit der Übertragungswege fehlen, entsprechende Vorschläge des Bundesrates hat die Bundesregierung abgelehnt.²⁵

Der Gesetzentwurf erweitert intrusive Cyberabwehrbefugnisse, ohne gleichzeitig die notwendigen Schutz-, Transparenz- und Governance-Mechanismen zu etablieren. Insbesondere beim Umgang mit Schwachstellen, der Dokumentation operativer Maßnahmen und der Sicherung digitaler Beweismittel bestehen Regelungs- oder Transparenzlücken. Ohne entsprechende Standards drohen sowohl rechtliche Unsicherheiten als auch Risiken für Transparenz, Kontrolle und gerichtliche Verwertbarkeit.

²⁵ [Deutscher Bundestag \(2026\): Unterrichtung durch die Bundesregierung – Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, BT-Drucksache 21/7406 vom 29.07.2026](#)

3. Empfehlungen

Systematische Evaluierung einführen: Jede Maßnahme der Cyberabwehr sollte messbare Sicherheitsgewinne dokumentieren. So lassen sich politische und operative Entscheidungen transparent begründen. Nur auf dieser Basis können Wirksamkeit und Bedarf realistisch bewertet werden.

Verhältnismäßige Maßnahmen: Intrusive Eingriffe sollten auf das notwendige Minimum beschränkt werden. Effizienz, Wirksamkeit und Eskalationsrisiko sind zu prüfen, Risiken von Kollateralschäden und Werkzeugproliferation zu bewerten und die Kosten aktiver Cyberabwehr gegen die Risiken des Nicht-Handelns abzuwägen. Die Eingriffsschwellen für BKA und BPol sollten mindestens an die des BSI angeglichen werden: Maßnahmen nach BKAG-E §§ 68b–68d und BPolG-E § 41a sollten eine erhebliche Gefahr voraussetzen.

Verfassungsrechtliche Klarheit schaffen: Zuständigkeiten zwischen Bund und Ländern müssen eindeutig geregelt werden. Eine offene Grundsatzdebatte über BKA-Befugnisse und gegebenenfalls eine Grundgesetzänderung ist dafür erforderlich.

Operative Plattform etablieren: Alle relevanten Behörden müssen auf einer gemeinsamen Ebene planen und operative Maßnahmen koordinieren können. Nur so lassen sich Doppelstrukturen vermeiden und Effizienzgewinne realisieren.

Koordination sicherstellen: Einheitliche Abstimmungs- und Konfliktlösungsmechanismen (*Deconflicting*) zwischen BKA, BPol, BSI, BfV, BND, Bundeswehr und den Länderpolizeien sind notwendig. Dies schafft Klarheit bei Verantwortlichkeiten und verhindert zersplitterte Vorgehensweisen.

Personelle Kapazitäten erhöhen: Die Stellen für Threat Hunting und Vorfallsbearbeitung beim BSI sollten deutlich ausgebaut werden. Gleichzeitig ist die operative Handlungsfähigkeit strategisch zu stärken, um IT-Sicherheit und Resilienz effektiv zu erhöhen.

Transparenz und Schutzmechanismen stärken: Für intrusive Cyberabwehrbefugnisse sollten klare Regeln für Beschaffung, Nutzung und Verwaltung von Schwachstellen, Exploits und technischen Werkzeugen festgelegt sowie ein regelmäßiges Berichtssystem über angeordnete, genehmigte und durchgeführte Maßnahmen eingeführt werden. Eingriffe nach BKAG-E § 68d und BPolG-E § 41a (1) Satz 1 Nummer 3 sollten unabhängig von der Nutzungsart des Systems einem Richtervorbehalt unterliegen und vollständig protokolliert werden. Die von der Bundesregierung angekündigte Ergänzung des BKAG § 90 zur gerichtlichen Zuständigkeit

interface I

sollte im parlamentarischen Verfahren tatsächlich erfolgen. Ergänzend sind verbindliche technische Standards und Governance-Mechanismen erforderlich, um die Integrität digitaler Beweismittel und die gerichtliche Verwertbarkeit sicherzustellen; sofern vorhanden, sollten entsprechende Hinweise in den Gesetzesfolgen aufgenommen werden.