



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

Schriftliche Stellungnahme

von Prof. Dr. Haya Schulmann, Goethe-Universität 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
Innenausschuss
Platz der Republik 1
11011 Berlin

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (BT-Drucksache 21/6585)

Schriftliche Stellungnahme zur öffentlichen Anhörung des Innenausschusses

Der Entwurf gibt der aktiven Cyberabwehr die Rechtsgrundlage, die bislang zu einem großen Teil fehlte; ich begrüße ihn. Aktive Cyberabwehr braucht dreierlei: ein Lagebild, das auch die Infrastruktur der Angreifer erfasst, Maßnahmen im Netz, die den Schaden begrenzen, und als letztes Mittel den Eingriff in Systeme der Angreifer. Der Entwurf regelt das Zweite und das Dritte. Für das Erste erweitert er die Datenquellen des BSI; einen gesetzlichen Auftrag, daraus ein Lagebild zu erstellen, das die Infrastruktur der Angreifer einschließt, gibt er nicht. Ich empfehle, diesen Auftrag ins Gesetz zu schreiben, die Maßnahmen im Netz technisch nachzuschärfen und das Eindringen in fremde Systeme stärker zu sichern.

1. Oktober 2026

**Fachbereich Mathematik
und Informatik (FB12)**

Institut für Informatik

Prof. Dr. Haya Schulmann

Besucheradresse
Robert-Mayer-Straße 10
60325 Frankfurt am Main

Postadresse
60629 Frankfurt am Main
Germany

schulmann@em.uni-frankfurt.de
cyber.informatik.uni-frankfurt.de

Vorrede

Im Januar 2021 haben das Bundeskriminalamt und die Generalstaatsanwaltschaft Frankfurt am Main die Steuerungsserver des Botnetzes Emotet übernommen und die Schadsoftware auf den Rechnern der Opfer deaktiviert. Die Operation gilt als Erfolg. Ob es für sie eine belastbare Rechtsgrundlage gab, wurde schon damals bezweifelt.¹ Der Entwurf schafft diese Grundlage für die Gefahrenabwehr. Er setzt zuerst im Netz an, bei Umleitung, Sperrung und Anordnungen an Anbieter und Registries. Nichts im Entwurf gestattet es, einem Angreifer mehr Schaden zuzufügen, als die Abwehr der Gefahr verlangt. Ich begrüße den Entwurf.

Wirken können die neuen Befugnisse aber nur, wenn jemand weiß, wogegen sie zu richten sind, was ein frühzeitiges Erkennen von Angreiferaktivitäten voraussetzt. Dafür tut der Entwurf zu wenig, er regelt das Erkennen nur in Teilen.

1 Was aktive Cyberabwehr ist und weshalb man sie braucht

1.1 Was wir haben, reicht nicht

Warum es auf das Erkennen ankommt, zeigt die Lage. Das BSI zählte im Berichtszeitraum 2025 täglich 119 neue Schwachstellen, rund 24 % mehr als im Jahr davor, und die Ausnutzung von Schwachstellen nahm um 38 % zu.² Der Bitkom beziffert den Schaden der deutschen Wirtschaft durch Cyberangriffe für 2025 auf 202,4 Milliarden Euro, nach 178,6 Milliarden im Jahr davor. Für 2026 weist er einen Korridor von 160,4 bis 205,8 Milliarden aus.³ Sicherheit und guter Betrieb bleiben unverzichtbar: IT modernisieren, Schwachstellen schließen, Zugänge mit mehr als einem Faktor sichern, wie es § 30 BSIg seit Dezember 2025 von wichtigen und besonders wichtigen Einrichtungen verlangt.⁴ Eine Garantie, dass alle Angriffe erfolglos bleiben, ist das nicht, aus drei Gründen.

Erstens gibt es Angriffe, die außerhalb des eigenen Bereichs stattfinden, wie Denial-of-Service-Angriffe und Verkehrsumleitungen im Internet.

Zweitens kontrolliert kein Betreiber alles, wovon seine Sicherheit abhängt. Schon einzelne Geräte enthalten Software verschiedener Hersteller. Die Firmware eines Routers enthält zahlreiche Fremdkomponenten, deren Pflege und Aktualisierung von weiteren Akteuren abhängen. Eine Studie von Zhao u. a. mit einem Datensatz von 34.136 Firmware-Abbildern verschiedener IoT-Geräte ermittelte für die untersuchten Drittkomponenten einen durchschnittlichen Versionsrückstand von rund 5,3 Jahren gegenüber der bei Veröffentlichung der jeweiligen Firmware neuesten verfügbaren Komponentenversion.⁵ In unserer eigenen Erhebung betrafen 78,9 % der in Patchnotes genannten unterschiedlichen CVEs Drittsoftware. Zugleich gaben nur 5 von 17 untersuchten Router-Herstellern einen bezifferten Unterstützungszeitraum an.⁶ Solche Abhängigkeiten bestehen auch im laufenden IT-Betrieb beim Hosting, bei Cloud-Diensten und bei anderen externen IT-Dienstleistungen. Auch diese Anbieter sind Teil der digitalen Lieferkette, und von ihrer Sicherheit hängt die Sicherheit der Betreiber mit ab. Wie groß der Anteil extern betriebener Infrastruktur sein kann, zeigt unsere Un-

¹Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Aktive Cyberabwehr, Impulspapier, März 2023 (im Folgenden: Impulspapier), S. 5; es beruht auf Haya Schulmann / Michael Waidner, Der Weg zur aktiven Cyberabwehr, FAZ vom 25. April 2022, S. 18; ausführlicher dies., Aktive Cyberabwehr, DuD 47 (2023), S. 497–502.

²BSI, Die Lage der IT-Sicherheit in Deutschland 2025, Kurzfassung, S. 3 und 7.

³Bitkom, Wirtschaftsschutz 2025, Pressemitteilung vom 18. September 2025, und Wirtschaftsschutz 2026, Pressemitteilung vom 26. August 2026; repräsentative Befragungen von jeweils rund 1.000 Unternehmen, hochgerechnet.

⁴BSIg in der Fassung des NIS2UmsuCG, BGBl. 2025 I Nr. 301, § 30 Abs. 2 Nr. 10, S. 22–23: Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung.

⁵B. Zhao u. a., One Bad Apple Spoils the Barrel: Understanding the Security Risks Introduced by Third-Party Components in IoT Firmware, IEEE TDSC 21(3), 2024, S. 1372–1389 (Zahlen nach der Preprint-Fassung, S. 1 und 13).

⁶ATHENE Erhebung und -Analyse, Datenstand August 2026.

tersuchung der staatlichen IT: Unsere Messung der von außen sichtbaren IT der Bundesministerien ordnet der Bundesverwaltung Ende 2025 rund 36.100 aktive IP-Adressen zu, davon mehr als 21.700, also über 60 %, extern beziehungsweise in der Cloud gehostet. Bei den Ländern wuchs das externe Hosting zwischen 2023 und 2025 um 88 %.⁷ Auch Webseiten hängen von Drittkomponenten und externen Diensten ab. Ein Beispiel sind eingebundene Skripte, die von fremden Servern geladen werden und deren Code die dortigen Anbieter jederzeit ändern können. Eine ATHENE-Auswertung des Common Crawl vom Oktober 2025 zeigt das Ausmaß dieser Abhängigkeiten: 1,81 Milliarden Seiten luden Skripte von 1,32 Millionen Hosts.⁸ Ein Betreiber kann seine eigenen Pflichten vollständig erfüllen und dennoch über Drittkomponenten oder externe Dienste angreifbar bleiben, deren Sicherheit er nur begrenzt überprüfen und beeinflussen kann.

Drittens suchen die Werkzeuge, mit denen Betreiber Angriffe erkennen, nach Bekanntem. Diese Suche kann kleinere Varianten des schon Bekannten mit abdecken, aber im Kern verglichen Virens Scanner Dateien mit Signaturen bekannter Schadsoftware, Systeme zur Angriffserkennung suchen im Netzverkehr nach Mustern früherer Angriffe, Filter sperren Adressen, die schon einmal aufgefallen sind. Gegen den nächsten Angriff hilft das nur begrenzt. Das BSI zählte zuletzt täglich rund 280.000 neue Varianten von Schadprogrammen und schreibt dazu: „Neue Malware-Varianten werden oft automatisch erzeugt, um signaturbasierter Detektion zu entgehen.“⁹ Professionelle Angreifer gehen weiter. Sie klären ihr Ziel vorher auf, seine Schutzmechanismen eingeschlossen, und richten ihre Werkzeuge darauf ein. Die Schadsoftware, die 2020 über signierte Updates der Firma SolarWinds zu „fewer than 18,000“ Kunden kam, wartete nach der Installation bis zu zwei Wochen, tarnte ihren Netzverkehr als den des Herstellers und prüfte, ob Virens Scanner und Forensikwerkzeuge liefen.¹⁰ Entdeckt hat sie FireEye, eines der führenden Sicherheitsunternehmen, das kurz zuvor den Diebstahl seiner eigenen Angriffswerkzeuge gemeldet hatte.

Getroffen werden also auch die, die am meisten von Sicherheit verstehen. Als häufigsten Grund dafür, dass ein Angriff zum Schaden führte, nannten 59 % der geschädigten Unternehmen 2026 die unzureichende Erkennung von Sicherheitsvorfällen.¹¹ Die eigene Sicherheit zu verbessern und nach den Mustern früherer Vorfälle zu suchen, bleibt nötig, genügt aber nicht.

1.2 Man braucht Lagebilder der Angreifer und Abwehr an ihrer Infrastruktur

Die übliche Antwort auf einen erkannten Angriff findet beim Opfer statt: den befallenen Server vom Netz nehmen, Zugangsdaten widerrufen, das System neu aufsetzen. Das ist klassische IT-Sicherheit. Bei manchen Angriffen versagt diese Antwort, weil sie sich komplett außerhalb des Einflussbereichs der Opfer abspielen. Ein Überlastungsangriff verstopft die Leitung, bevor er die Systeme des Opfers erreicht. Aktive Cyberabwehr setzt deshalb auf der anderen Seite an. Wir haben sie 2022 so bestimmt: Sie umfasst „technische Maßnahmen, die Angriffe stoppen oder proaktiv verhindern sollen, indem sie in die Infrastrukturen oder digitalen Ressourcen der Angreifer eingreifen“.¹² Das reicht vom Umleiten und Sperren von Datenverkehr über das Abkoppeln von Domains und Servern und das Bereinigen befallener Opfersysteme bis zum Eindringen in Systeme, die für Angriffe genutzt werden.

Ein Angriff verläuft in Schritten. Typisch sind Aufklärung, Zustellung, Einnisten, Ausbreitung im

⁷H. Schulmann, ATHENE Cybernation Deutschland. Studie der externen Angriffsfläche: IT der Bundesministerien 2025, Goethe-Universität Frankfurt, Juli 2026, S. 4; dies., Sicherheit der IT der Länder. Studie der externen Angriffsfläche der 16 Bundesländer (2023–2025), Januar 2026, S. 2.

⁸ATHENE-Messung (2025).

⁹BSI, Die Lage der IT-Sicherheit in Deutschland 2025, Abschnitt Bedrohungen (Webfassung).

¹⁰SolarWinds Corp., Form 8-K vom 14. Dezember 2020, Item 8.01; FireEye, Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, 13. Dezember 2020; FireEye, Unauthorized Access of FireEye Red Team Tools, 8. Dezember 2020.

¹¹Bitkom, Wirtschaftsschutz 2026 (Fn. 3).

¹²Schulmann / Waidner, FAZ vom 25. April 2022 (Fn. 1); dort auch die vier Klassen.

Netz, Steuerung von außen, Ausleitung der Daten. Jeder Schritt verändert etwas, das sich beobachten lässt, und jeder lässt sich unterbrechen. Hutchins, Cloppert und Amin haben daraus 2011 den Kern der Verteidigung gemacht: „just one mitigation disrupts the chain and the adversary“.¹³ Je früher, desto leichter. CrowdStrike misst im Mittel 48 Minuten vom ersten Zugriff bis zur Ausbreitung im Netz. Bis zur Entdeckung vergehen nach Mandiant im Median 14 Tage.¹⁴ Mit KI wird es schneller. Google beschreibt Angreifer, die 2026 eine Cloud-Ressource übernahmen und eine agentengestützte Kampagne zum massenhaften Abgreifen von Zugangsdaten „in under six hours“ planten, bauten und ausführten.¹⁵

Für fast alle diese Schritte braucht der Angreifer Infrastruktur außerhalb des Opfers: Domains, Server zum Nachladen und Steuern, Konten, Speicher für die Beute. Er muss sie mieten, registrieren und mit Zertifikaten versehen, bevor der Angriff beginnt, und das hinterlässt Spuren. Deshalb lohnt es sich, diese Infrastruktur abzuschalten. Ihr Wiederaufbau kostet den Angreifer Zeit und Geld, und er nutzt sie meist lange und für mehr als einen Angriff.¹⁶ Ist sie ausgeschaltet, steht der laufende Angriff, und dem nächsten fehlt die Grundlage. Ob Angreifer die Infrastruktur danach neu aufbauen und wie lange das dauert, kann man nicht allgemein vorhersagen. Emotet war rund zehn Monate nach dem Takedown zurück.¹⁷

Voraussetzung ist, dass man die Infrastruktur kennt, bevor der Schaden eintritt. Dafür braucht es zwei Lagebilder: eines der eigenen IT und eines der Gegenseite, also der Infrastruktur, die Angreifer aufbauen, mieten oder kapern.¹⁸

Dass das zweite Lagebild möglich ist, haben wir gezeigt. Beispielsweise haben wir über drei Jahre bis zu 3,1 Millionen Domains und Subdomains wöchentlich von außen abgerufen und die Veränderungen an Namenseinträgen und Inhalten ausgewertet. So fanden wir 20.904 Übernahmen aufgegebenen Cloud-Ressourcen, bei Verwaltungen, Universitäten und 31 % der Fortune-500-Unternehmen, ordneten sie 1.798 Gruppen zusammengehöriger Infrastruktur zu und benachrichtigten mehr als 300 betroffene Organisationen. Den Herstellern von Schutzsoftware war fast keine dieser Domains bekannt. Von 17.698 stufte nur 135 mindestens einer als schädlich ein.¹⁹ Wer Registrierungen, Namenseinträge, Zertifikate und eingebundene Skripte laufend beobachtet, sieht solche Veränderungen, kann die möglichen Opfer warnen und die Spur zu den Servern der Angreifer zurückverfolgen.

In der Praxis sollte die Erstellung dieses zweiten Lagebilds im Wesentlichen durch erkannte potenzielle Gefahren gesteuert werden: Stellt man einrichtungsübergreifend anomale Veränderungen in der IT der eigenen Einrichtungen fest, kann man deren Verursacher feststellen und so Hinweise auf mögliche von Angreifern genutzte entfernte Infrastrukturen erhalten. Die Daten aus deren Beobachtung kann man weiter mit den Daten der eigenen Einrichtungen und öffentlichen Daten korrelieren und so die Indizien für einen Angriff weiter verdichten.

Der Angriff auf das Berliner Landesnetz im August 2026 zeigt, was von einem zweiten Lagebild abhängt. Laut der Warnung des BSI beginnt die Kampagne an einer kompromittierten Webseite. Ein gefälschtes CAPTCHA bringt den Nutzer dazu, selbst einen Befehl auszuführen. Es folgen das Nachladen von Servern der Angreifer, das Ausspähen des Netzes, ein Tunnel nach außen und der

¹³E. M. Hutchins, M. J. Cloppert, R. M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin, 2011, S. 2.

¹⁴CrowdStrike, 2025 Global Threat Report, S. 12; Mandiant, *M-Trends 2026*, Executive Edition, S. 2–3.

¹⁵Google Threat Intelligence Group, *GTIG AI Threat Tracker: From Prompting to Autonomy*, 8. September 2026.

¹⁶Haya Schulmann / Michael Waidner, *Cyberabwehr beginnt vor dem Angriff*, FAZ vom 30. März 2026, S. 20: „Der Aufbau einer Infrastruktur ist aufwendig und teuer.“ Sie bleibe deshalb häufig über längere Zeit aktiv.

¹⁷Palo Alto Networks Unit 42, *Emotet Summary: November 2021 Through January 2022*.

¹⁸Schulmann / Waidner, FAZ vom 30. März 2026 (Fn. 16): „Wer aktive Cyberabwehr betreiben will, braucht übrigens zwei Lagebilder.“

¹⁹J. Frieß, T. Gattermayer, N. Gelernter, H. Schulmann, M. Waidner, *Cloudy with a Chance of Cyberattacks: Dangling Resources Abuse on Cloud Platforms*, USENIX NSDI 2024, S. 1977–1994, hier S. 1978–1982 und 1986–1988.

Abfluss der Daten.²⁰ In Berlin floss der wesentliche Teil der Daten vom 7. bis 12. August ab. Vom Netz getrennt wurden die betroffenen Senatsverwaltungen erst am 14. August.²¹ Aktive Cyberabwehr, die unsere Methode nutzt, hätte die kompromittierte Webseite frühzeitig erkennen und den Angriff unterbrechen können. Tatsächlich haben wir mit unserer Methode 2025 Dutzende laufender Angriffe dieser Art erkannt und verhindert, darunter auch einen Angriff auf ein Landesministerium.²²

Wie Webseiten in fremde Hand geraten, lässt sich an vielen Beispielen nachvollziehen. Eine Skriptquelle wird verkauft, ein Dienstleister gibt eine Ressource auf, Angreifer übernehmen einen Namineintrag oder dringen beim Dienstleister ein. Polyfill.io, eine Domain, von der mehr als 100.000 Websites ein Skript luden, wurde im Februar 2024 verkauft und lieferte danach Schadcode aus. Cloudflare hatte knapp vier Monate vor dem ersten Bericht darüber öffentlich vor diesem Risiko gewarnt.²³ In einem anderen Fall erkannte unser Monitoring, dass ein deutscher Website-Dienstleister einen Cloud-Speicher gelöscht hatte, aus dem acht Webanwendungen öffentlicher Einrichtungen weiter Code luden. Dies erlaubte Angreifern, den Namen selbst neu zu registrieren und so Schadcode zu verteilen. Nach unserer Meldung sicherte der Cloud-Anbieter die Ressource.²⁴ In solchen Fällen kann der Nutzer alles richtig machen und wird trotzdem angegriffen, weil der Fehler außerhalb seines Netzes liegt. Von außen ist er sichtbar. Das Skript des gefälschten CAPTCHA fand das BSI nachträglich „in historischen Daten auf mehreren Hundert Webseiten“.²⁵

Genau solche Veränderungen findet das Monitoring, das wir beschrieben haben, proaktiv. Es ruft die beobachteten Seiten regelmäßig ab, vergleicht die Abbilder und schlägt an, wenn binnen kurzer Zeit auf vielen Seiten derselbe neue Inhalt erscheint, auch ein eingebundenes Skript.²⁶ Der Angriff auf die Bundesbehörde und der auf das Berliner Landesnetz wären damit an ihrem Ausgangspunkt erkennbar gewesen, sofern die benutzten Seiten zum beobachteten Bestand gehören. Wer eine solche Seite früh findet, kann ihren Betreiber warnen, sie sperren lassen und mit denselben Merkmalen weitere finden; wer die Server dahinter kennt, kann Tunnel und Abfluss unterbrechen.

Aktive Cyberabwehr besteht aus drei Aufgaben. Erstens das Lagebild: wissen, was sich an der eigenen Angriffsfläche verändert und Lokalisierung der Infrastruktur der Angreifer. Zweitens die Schadensbegrenzung: warnen, umleiten, sperren, ohne in fremde Systeme einzudringen. Drittens: die Infrastruktur der Angreifer außer Betrieb setzen, über ihre Anbieter oder, als letztes Mittel, durch den Eingriff in das System selbst.

2 Was dafür geregelt sein muss

Jede der drei Aufgaben braucht im Gesetz eine Zuständigkeit, Befugnisse mit einem Anwendungsbereich und Sicherungen. Die folgende Übersicht zeigt, was gilt und was der Entwurf hinzufügt. Neu ist in der Spalte des BSI, was auf das Wort „Neu“ folgt; neu sind auch alle Befugnisse von BKA und Bundespolizei (§§ 68a bis 68f BKAG-E, § 41a BPolG-E) mit ihren Sicherungen.

²⁰BSI, Deutsche Institutionen über TerminalFix-Kampagne kompromittiert, BITS-B Nr. 2026-287419-1032, 4. September 2026, S. 1–2; die Verbindung zum Berliner Vorfall zieht das BSI in einem Beitrag auf social.bund.de vom selben Tag.

²¹Senatskanzlei Berlin, Cyberangriff auf das Landesnetz: Informationen für Bürgerinnen und Bürger, Stand 29. September 2026.

²²ATHENE Messungen.

²³Sansec, Polyfill supply chain attack hits 100K+ sites, 25. Juni 2024; Cloudflare, polyfill.io now available on cdnjs: reduce your supply chain risk, 29. Februar 2024.

²⁴ATHENE Messungen.

²⁵BSI-Warnung (Fn. 20), S. 2.

²⁶Frieß u. a., NSDI 2024 (Fn. 19), Abschnitt 3.

Aufgabe	BSI	BKA und Bundespolizei	Sicherungen
Lagebild	Lagebild für kritische Anlagen und NIS-2-Einrichtungen (§ 40 Abs. 3 Nr. 3 BSIg); Meldestelle und Protokolldaten des Bundes (§§ 4, 8, 9); Abfragen von außen und Honeypots (§ 15 Abs. 1 und 5); Meldepflichten (§ 32). Neu: Indikatoren der KRITIS-Betreiber (§ 31 Abs. 3 BSIg-E), Auskünfte der Anbieter (§ 15 Abs. 6), Liste gefährlicher Domains (§ 16 Abs. 6)	Nur im Einzelfall einer Gefahr: umgeleiteten Verkehr aufzeichnen (§ 68c Abs. 1 BKAG-E; § 41a Abs. 1 Nr. 2 BPolG-E), Daten auslesen (§ 68d; § 41a Abs. 1 Nr. 3)	Zweckbindung; Pseudonymisierung der Protokolldaten; Höchstfristen von 18 und, neu, 24 Monaten
Schadensbegrenzung	Verantwortliche informieren und warnen (§ 15 Abs. 2, § 13 BSIg); Anordnungen an TK-Anbieter (§ 16). Neu: an Registries (§ 16a BSIg-E) und an Cloud-, CDN-, Rechenzentrums- und Managed-Service-Anbieter (§ 17 Abs. 2); DNS-Filter (§ 16 Abs. 7)	Verkehr einschränken, unterbinden, umleiten, auch durch Anordnung an Anbieter (§ 68c; § 41a Abs. 1 Nr. 2, Abs. 9)	BSI: erhebliche Gefahr, Benehmen mit der Bundesnetzagentur. Polizei: Gefahr im Einzelfall, Benehmen mit dem BSI
Infrastruktur der Angreifer außer Betrieb setzen	Neu: eine Domain über die Registry abkoppeln lassen (§ 16a BSIg-E). Kein eigener Eingriff in fremde Systeme; nur Bereinigungsbefehle an befallene Opfersysteme (§ 16 Abs. 1 Nr. 2, Abs. 2 BSIg)	Betrieb untersagen (§ 68b; § 41a Abs. 1 Nr. 1); gefahrgegenständliche Daten auslesen, löschen, verändern, auch durch Eindringen (§ 68d; § 41a Abs. 1 Nr. 3)	Richtervorbehalt nur für Eingriffe in private Systeme, die eine Datenerhebung ermöglichen (§ 68e; § 41a Abs. 5 und 6); Rückgängigmachung, „soweit dies technisch möglich ist“; Kontrolle durch die Datenschutzaufsicht des Bundes (§ 69 BKAG)

Zuständig ist das BKA in drei Fällen: bei schwerwiegenden Gefahren, die nur gemeinsam mit anderen Staaten abzuwehren sind, bei Gefahren für die Funktionsfähigkeit von Behörden und Einrichtungen des Bundes und bei Gefahren für die Stellung der Bundesrepublik in der Staatengemeinschaft oder für die Verteidigung (§ 3a Abs. 1 BKAG-E). Im Übrigen bleiben die Länder zuständig. Das BKA unterstützt sie auf Ersuchen (§ 2 Abs. 5 Nr. 5), nach der Begründung aber nur, wenn „sowohl das ersuchende Land als auch das BKA über entsprechende Befugnisse zur Abwehr von Cybergefahren verfügen“.²⁷ Die Bundespolizei erhält die Befugnisse für ihre eigenen Aufgaben. Die Begründung nennt Grenzkontrollsysteme und die Bahn.²⁸

Für operative Konflikte zwischen den drei Behörden kennt der Entwurf ein einziges Instrument. Vor einer angeordneten Umleitung setzen sich BKA und Bundespolizei mit dem BSI ins Benehmen (§ 68c Abs. 3 BKAG-E, § 41a Abs. 10 BPolG-E), damit dort ein „Gesamtüberblick über Umleitungsmaßnahmen“ bleibt.²⁹ Ob dies genügt, um sich gegenseitig störende Aktionen zu verhindern, bleibt abzuwarten. Denkbar wäre etwa Folgendes: Das BSI sperrt eine Domain, deren Verkehr das BKA umleiten will, um befallene Geräte zu finden. Ein Anbieter müsste seine Nutzer warnen (§ 19 Abs. 5

²⁷BT-Drs. 21/6585, S. 16–17 und 19–21 (Normtext), Begründung S. 59.

²⁸BT-Drs. 21/6585, S. 7–9 (§ 41a BPolG-E), Begründung S. 43.

²⁹BT-Drs. 21/6585, Begründung S. 49 und 65.

und 6 TDDDG-E), während ihm das BKA die Offenlegung untersagt (§ 68f BKAG-E). Das Bereinigen eines Systems vernichtet Spuren, die die Strafverfolgung braucht.

Hinzu kommen die Nachrichtendienste. Die Reform des Nachrichtendienstrechts, die parallel beraten wird, erlaubt dem Verfassungsschutz und dem BND, bei informationstechnischen Angriffen Auskünfte von Anbietern zu verlangen. Aufzuklären sind dabei „die zum Angriff genutzte Infrastruktur und Technik sowie das Vorgehen und die Angriffsziele“.³⁰ Wer bei einer zusammenhängenden Operation führt, an der BSI, Polizei, Dienste, Länder und Anbieter beteiligt sind, sagt der vorliegende Entwurf nicht. Das Nationale Cyber-Abwehrzentrum wäre eine naheliegende Koordinierungsstelle, kommt aber im Entwurf nicht vor.

3 Einschätzung der Wirksamkeit der Maßnahmen im Entwurf

3.1 Für das Lagebild bringt er mehr Daten, aber keinen Auftrag

Im Gesetzestext des Entwurfs kommt das Wort Lagebild nicht vor, in der Begründung steht es dreimal: beim Personalbedarf des BKA („Erstellung von Lagebildern und Prognosen zu Cyber-Bedrohungen“), bei den Indikatoren aus kritischen Anlagen, die das BSI „zur Aggregation eines Echtzeitlagebildes“ nutzen soll, und beim Bußgeld im Energierecht. Die Meldungen aus diesen Anlagen sollen außerdem „für eine Lagedarstellung aufbereitet werden“.³¹ Was der Entwurf regelt, sind Datenquellen. Betreiber kritischer Anlagen übermitteln dem BSI künftig laufend Verfügbarkeits- und Angriffsindikatoren (§ 31 Abs. 3 BSIG-E). Telekommunikations- und Digitaldiensteanbieter müssen ggf. Auskunft über Schadaktivitäten, Schwachstellen und Bedrohungen geben (§ 15 Abs. 6), nach der Begründung auch über „DNS-Anfragedaten“. Umgeleitete Daten darf das BSI 24 statt bisher drei Monate behalten (§ 16 Abs. 5).³² Das ist ein Fortschritt. Die Angriffserkennung der kritischen Anlagen wird erstmals an das BSI angebunden, und die Datenbasis wächst. Der Entwurf bindet die Daten an die Aufgaben des BSI. Der eigentliche Auftrag, also dass das BSI aus all diesen und weiteren Daten ein Lagebild der Angreifer erstellen soll, steht nicht im Gesetz.

Auch das bislang geltende Recht kennt das Lagebild nur zur Hälfte. Das BSI hat „das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren“ (§ 40 Abs. 3 Nr. 3 BSIG), es sammelt für die Bundesverwaltung Meldungen und Protokolldaten, und es darf öffentlich erreichbare Systeme von außen abfragen.³³ Das alles betrifft die eigene Lage. Allgemein soll das BSI Informationen über Sicherheitsrisiken und Angriffe sammeln und auswerten (§ 3 Abs. 1 Satz 2 Nr. 2, § 40 Abs. 3 Nr. 1 BSIG). Einen ausdrücklichen Auftrag, den Aufbau von Angreiferinfrastruktur laufend zu beobachten, hat es nicht. Ebenso dürften viele der dafür notwendigen Befugnisse fehlen. Die Aufklärung der zum Angriff genutzten Infrastruktur ordnet die Nachrichtendienstreform dem Verfassungsschutz und dem BND zu (Fn. 30). Die Zusammenführung steht bisher nur in der alten Nationalen Sicherheitsstrategie von 2023: „Die Bundesregierung veranlasst, dass alle maßgeblichen Akteure zu einem ganzheitlichen Cyberlagebild beitragen.“³⁴ Im BSI-Gesetz steht davon nichts.

³⁰Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts, BR-Drs. 453/26, § 12 BVerfSchG-E, S. 17–18; ähnlich § 14 BNDG-E, S. 92–93.

³¹BT-Drs. 21/6585, S. 28, 29, 56 und 70.

³²BT-Drs. 21/6585, S. 12–15 (Normtext), Begründung S. 52–54.

³³BGBI. 2025 I Nr. 301, §§ 4, 8, 9 und 15 (S. 9–16), § 40 (S. 28).

³⁴Bundesregierung, Nationale Sicherheitsstrategie, Juni 2023, S. 61; die Koordinierungsfunktion werde „zunächst im Nationalen Cyberabwehrzentrum“ eingerichtet.

Baustein	Was der Entwurf leistet	Was fehlt
Lagebild der eigenen IT	Indikatoren der KRITIS-Betreiber (§ 31 Abs. 3 BSIG-E, § 5c Abs. 7 EnWG-E); Protokolldaten des Bundes, jetzt auch URLs (§ 8); Suche nach Angriffsspuren auf Ersuchen (§ 11)	Laufende Indikatoren liefern nur die kritischen Anlagen; die übrigen NIS-2-Einrichtungen melden Vorfälle (§ 32 BSIG), Länder und Kommunen sind nicht erfasst. Die Abfragen von außen bleiben an den Schutz der IT des Bundes gebunden (§ 15 Abs. 1 BSIG), und das Register der Einrichtungen führt IP-Adressbereiche, keine Domainnamen (§ 33)
Lagebild der Gegenseite	Liste gefährlicher Domains (§ 16 Abs. 6); Sinkhole-Daten 24 Monate (§ 16 Abs. 5); Auskünfte der Anbieter (§ 15 Abs. 6); die Polizei zeichnet umgeleiteten Verkehr auf (§ 68c BKAG-E)	Sinkhole-Daten und Aufzeichnungen setzen eine schon erkannte Gefahr voraus; Auskünfte und Domainliste geben wieder, was Anbieter und Hinweisgeber bereits wissen. Niemand hat den Auftrag, Registrierungen, Zertifikate und Skripte selbst laufend zu beobachten
Vorbereitung erkennen	Die Begründung sieht den Bedarf: Aufklärung erfordere „in der Regel eine mittel- bis langfristige Befassung“ (S. 30). Im System des Opfers darf das BSI künftig schon bei Anhaltspunkten für Vorbereitungen nach Spuren suchen, auf Ersuchen und in herausgehobenen Fällen (§ 11)	Vorbereitungen außerhalb der Opfersysteme beobachtet niemand laufend: neu registrierte Domains, gemietete Server, ausgestellte Zertifikate
Geteiltes Lagebild	Benennen vor Umleitungen; Übermittlungen an die Bundeswehr (§ 68a Abs. 4 BKAG-E, § 41a Abs. 13 BPolG-E)	Die Länder erhalten Informationen über ihre Kontaktstellen (§ 40 Abs. 3 Nr. 4 BSIG), tragen aber nichts Verpflichtendes bei; eine gemeinsame Plattform fehlt, und niemand ist für das Gesamtlagebild zuständig
Rückkanal zu den Betroffenen	Angriffserkennungssysteme „sollten“ BSI-Indikatoren verarbeiten können (§ 31 Abs. 2); Anbieter geben Warnungen an Nutzer weiter (§ 19 TDDDG-E); DNS-Filter (§ 16 Abs. 7)	Die Verarbeitung ist nur eine Soll-Vorgabe; abgestimmte Reaktionsabläufe (Playbooks) fehlen

Die Höchstfrist für umgeleitete Daten steigt auf 24 Monate. Das ist ein plausibler Wert. Nach der Begründung wurde das BSI „in der Mehrheit der bisher aufgetretenen Fälle erst über 12 Monate nach einem Vorfall von Partnerbehörden wie BKA, BfV kontaktiert“, und unsere eigene Messung beruht auf drei Jahren Historie.³⁵ Auf die Protokolldaten des Bundes dagegen darf das BSI nach drei Monaten nur noch zugreifen, wenn tatsächliche Erkenntnisse vorliegen, „dass der Bund von einem Schadprogramm oder einer sonstigen erheblichen Gefahr für seine Kommunikationstechnik betroffen ist“ (§ 8 Abs. 2 BSIG-E).³⁶ Die Auswertung selbst bleibt automatisiert zulässig. Ob dazu auch die Suche mit einem neuen Indikator in den älteren Daten gehört, lässt der Wortlaut offen; zählt sie als Zugriff, fehlt dem BSI genau die Erkenntnis, die es mit der Suche erst gewinnen will. Gerade die älteren Daten zählen aber. Mandiant misst für Spionagefälle eine Verweildauer von im Median 122 Tagen.³⁷

Ein Lagebild der Gegenseite entsteht nicht aus Meldungen und Protokollen allein. Es braucht breite,

³⁵BT-Drs. 21/6585, Begründung S. 54.

³⁶BT-Drs. 21/6585, S. 11.

³⁷Mandiant, M-Trends 2026, Executive Edition, S. 3.

fortlaufende Beobachtung, lange vor einem Angriff und unabhängig davon, welche Angriffstechnik gerade verbreitet ist. Es verbindet viele Quellen: Registrierungen, Namenseinträge, Zertifikate, Webinhalte, Verkehrsdaten der Netzbetreiber, Meldungen der Betroffenen. Welche Merkmale eine Vorbereitung verraten, ändert sich mit den Angreifern. Das ist Forschungsarbeit und keine Routine. Dass erst die Zusammenschau zählt, zeigt SolarWinds. 2020 bemerkten das US-Justizministerium und zwei Sicherheitsunternehmen unabhängig voneinander Auffälligkeiten an Servern mit dieser Software. Jeder untersuchte seinen Fall, keiner fand die Ursache, und sie wussten nichts voneinander.³⁸ Die Anfragen der Schadsoftware an ihre Steuerungsdomain lagen derweil in Sammlungen passiver DNS-Daten, aber Forscher werteten sie erst nach der Entdeckung aus.³⁹ Ich halte es für wahrscheinlich, dass drei Meldungen über denselben Hersteller und diese DNS-Daten, an einer Stelle zusammengeführt, die Kampagne früher gezeigt hätten. Beweisen lässt sich das im Rückblick allerdings nicht.

Ein Teil dieser Beobachtung wäre dem BSI schon heute erlaubt. Zu den Abfragen nach § 15 Abs. 1 BSIG zählt die Begründung des Gesetzes, das die NIS-2-Richtlinie umgesetzt hat, ausdrücklich „webseiten- / domainbasierte Methoden“.⁴⁰ Drei Fragen sind offen: ob die Befugnis, die an den Schutz der IT des Bundes gebunden ist, auch Abfragen bei Ländern, Kommunen und Unternehmen trägt; ob sie den wiederholten Abruf und Vergleich von Webinhalten und deren Aufbewahrung über Jahre deckt; und wer die Ergebnisse mit den Erkenntnissen von Polizei und Nachrichtendiensten zusammenführt.

Je mehr das BSI sammelt, desto lohnender wird es selbst als Ziel. Für die Übermittlung aus den kritischen Anlagen soll der Stand der Technik eingehalten werden (§ 31 Abs. 5 BSIG-E). Für die Auskünfte der Anbieter hat der Bundesrat „Anforderungen an die Sicherheit der Übertragungswege“ verlangt. Die Bundesregierung lehnt das ab, „um die betroffenen Unternehmen nicht über Gebühr zu belasten“.⁴¹ Zur Sicherung des Bestands beim BSI selbst sagt der Entwurf nichts.

Was also fehlt, ist ein klarer gesetzlicher Auftrag an das BSI, ein fortlaufendes Lagebild zu erstellen, das die Infrastruktur der Angreifer einschließt, und eine Befugnis, die dafür nötigen Quellen zu erfassen.

3.2 Für die Abwehr wirkt der Entwurf, wo Angreifer eigene Infrastruktur brauchen

Wie weit die neuen Befugnisse ohne dieses Lagebild tragen, zeigen zwölf Fälle aus den vergangenen Jahren. Die Tabelle ordnet sie danach, ob der Entwurf hilft, teilweise hilft oder nicht reicht. Die rechte Spalte hält fest, ob der Angriff früh zu erkennen gewesen wäre. In elf der zwölf Fälle lag ein Signal vor, das früh erkennbar war oder das Dritte tatsächlich gesehen haben: in acht Fällen klar, in drei nur an bestimmten Stellen, etwa im Netz eines großen Betreibers. Die Daten waren also da, nur rechtzeitig ausgewertet hat sie niemand.

³⁸K. Zetter, DOJ Detected SolarWinds Breach Months Before Public Disclosure, Wired, 28. April 2023 (nach ungenannten Quellen; das Ministerium bestätigt Vorfall und Untersuchung); SolarWinds, New Findings From Our Investigation of SUNBURST, 11. Januar 2021.

³⁹I. Kuznetsov, C. Raiu (Kaspersky), Sunburst: connecting the dots in the DNS requests, 18. Dezember 2020.

⁴⁰BT-Drs. 21/1501, S. 141; zur Fassung des Innenausschusses BT-Drs. 21/2782, S. 19–20.

⁴¹BT-Drs. 21/7406, S. 2 und 5.

Fall	Was der Entwurf leistet	Grenze	Früh erkennbar?
1. Botnetz mit zentraler Steuerung (Emotet 2021, Qakbot 2023) ⁴²	Umleitung auf eigene Server (§§ 16, 16a, 17 Abs. 2 BSIG-E), Abschalten über die Anbieter (§ 68b BKAG-E), Deaktivieren auf den Opfersystemen (§ 68d)	Emotet war nach rund zehn Monaten zurück, Qakbot nach drei	Ja. Die Steuerungsserver waren bekannt; das US-Sensorsystem EINSTEIN meldete 2020 rund 16.000 Emotet-Alarme
2. Kompromittierte Webseite, z. B. übernommene Skriptquelle (Polyfill.io 2024) ⁴³	Anordnung an die Registry (§ 16a), Domainliste mit DNS-Filter (§ 16 Abs. 6 und 7), Anordnung an CDN-Anbieter (§ 17 Abs. 2)	Die Verweise bleiben: im Oktober 2025 noch 2,41 Millionen Seiten-URLs	Ja. Der Wechsel der Kontrolle war knapp vier Monate vorher öffentlich bekannt
3. Aufgegebene Cloud-Ressource (20.904 Übernahmen) ⁴⁴	Betreiber warnen (§ 15 Abs. 2 BSIG); Anordnung an den Cloud-Anbieter nur bei erheblicher Gefahr (§ 17 Abs. 2 BSIG-E)	Dauerhaft hilft nur, dass der Inhaber den verwaisten DNS-Eintrag löscht	Ja. Der verwaiste Eintrag ist von außen sichtbar, bevor jemand die Ressource übernimmt
4. Tarnnetz aus gekaperten Routern (Volt Typhoon, KV-Botnet 2024) ⁴⁵	Schadsoftware auf den Geräten entfernen (§ 68d BKAG-E), wie es das FBI getan hat	Veraltete Geräte werden neu infiziert; ob der Richtervorbehalt gilt, hängt an „privat genutzt“	Teilweise. Im Netz eines großen Betreibers sichtbar, beim Opfer kaum; in manchen Opfernetzen hielt der Zugang mindestens fünf Jahre
5. DDoS-Kampagne (NoName057(16)) ⁴⁶	Steuerungsserver abschalten, Angriffsverkehr umleiten (§§ 68b, 68c BKAG-E, § 16 BSIG)	Das trifft erst die nächste Welle; Takedowns wirkten bisher kurz	Ja, was die Ziele angeht. Der Steuerungsserver verteilt die Zielliste an jeden Teilnehmer
6. Infostealer und gestohlene Zugangsdaten (Snowflake 2024) ⁴⁷	Listen, Filter und Sinkholes stoppen die Verteilung und zeigen die Opfer	Die gestohlenen Zugangsdaten bleiben gültig, bis die Opfer sie ändern	Ja. Die Zugangsdaten lagen zum Teil seit 2020 in den Protokollen der Schadsoftware
7. TerminalFix-Kette gegen eine Bundesbehörde ⁴⁸	Das BKA ist zuständig (§ 3a Abs. 1 Nr. 2) und kann Tunnel und Abfluss kappen (§ 68c)	Die Ausbreitung im Netz dauert im Mittel 48 Minuten; den Zugriff auf ältere Protokolldaten bremst § 8 BSIG	Ja, am Ausgangspunkt. Das Köderskript stand auf mehreren hundert Websites; ein Monitoring der Webinhalte zeigt das. Nachladen und Tunnel sind im Netz sichtbar

⁴²Zur Rückkehr Unit 42 (Fn. 17) und The Register, Qakbot's backbot, 19. Dezember 2023; zur Erkennung CISA und MS-ISAC, Alert AA20-280A, Emotet Malware, Oktober 2020.

⁴³Sansec und Cloudflare (Fn. 23); die Zahl von 2025 nach eigener Messung (Fn. 8).

⁴⁴Frieß u. a., NSDI 2024 (Fn. 19).

⁴⁵U.S. District Court S.D. Tex., 4:23-mc-5530 (KV-Botnet); Black Lotus Labs (Lumen), Routers roasting on an open firewall: the KV-botnet investigation, Dezember 2023; CISA u. a., Advisory AA24-038A, 7. Februar 2024.

⁴⁶BKA und ZIT, Pressemitteilung zu Operation Eastwood, 16. Juli 2025: seit November 2023 14 Angriffswellen gegen rund 250 Unternehmen und Einrichtungen in Deutschland; Sekoia, Following NoName057(16) DDoS Project's Targets, 29. Juni 2023.

⁴⁷Mandiant, UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, 10. Juni 2024: rund 165 Organisationen benachrichtigt; mindestens 79,7 % der genutzten Konten waren vorher offengelegt, die früheste Infektion datiert vom November 2020.

⁴⁸BSI-Warnung (Fn. 20); zu den Zeiten Fn. 14.

Fall	Was der Entwurf leistet	Grenze	Früh erkennbar?
8. Derselbe Angriff auf ein Landesnetz (Berlin 2026) ⁴⁹	Es bleiben die Anordnungen des BSI (§§ 16, 16a); das BKA hilft in der Regel nur auf Ersuchen	Zuständig ist in der Regel das Land; die Leak-Seite im Tor-Netz erreicht keine Maßnahme	Ja, am Ausgangspunkt wie in Fall 7. Der Abfluss dauerte sechs Tage; der Erstzugriff ist nicht öffentlich
9. Softwarelieferkette (SolarWinds 2020) ⁵⁰	Bis zur Entdeckung gibt es nichts, wogegen sich eine Befugnis richten könnte; danach lässt sich die Steuerung angreifen wie in Fall 1. Mit einem Auftrag an das BSI zur umfassenden Lagebilderstellung könnten entsprechende Kampagnen entdeckt werden	Der Schadcode kam im signierten Update des Herstellers	Teilweise. Die Hintertür nicht, die Kampagne über DNS-Daten und Einzelmeldungen
10. Zugang über das VPN (Südwestfalen-IT 2023) ⁵¹	Die Täter verbanden sich direkt über ein verwundbares VPN ohne zweiten Faktor; eine Infrastruktur, an der Netzmaßnahmen ansetzen könnten, ist nicht bekannt. Auch hier: Es fehlte ein erweiterter Auftrag an das BSI.	Zuständig wäre das Land	Ja. Der Angriff lief elf Tage; schon am ersten Tag gab es 380 fehlgeschlagene Anmeldungen an 190 Servern
11. Zerstörung in Stunden (Viasat KA-SAT 2022) ⁵²	Erkennen, Anordnen und Abschalten dauern länger als der Angriff	Angriff nutzte bereits vorhandene Kompromittierung aus	Kaum. Zwischen den ersten Anmeldeversuchen und der Wirkung lagen Stunden
12. Spione im Telekommunikationsnetz (Salt Typhoon) ⁵³	Umleiten und Sperren setzen voraus, dass die Netze vertrauenswürdig sind	Die Angreifer sitzen bei den Betreibern, die die Anordnungen ausführen sollen	Teilweise. Der Einstieg lief über bekannte Schwachstellen; danach hilft nur die Überwachung der Gerätekonfiguration

Der Entwurf wirkt also dort, wo der Angreifer auf Infrastruktur angewiesen ist, die sich finden und über Anbieter oder Registries erreichen lässt. Er genügt nicht, wo es diese Infrastruktur nicht gibt oder niemand sie kennt, wo der Angriff in Stunden abläuft oder wo ein Land zuständig ist. Gerade dort kommt es auf das Erkennen an. Bei der Südwestfalen-IT hat erst die Forensik die auffälligen Protokolleinträge des ersten Tages ausgewertet.

Die Maßnahmen im Netz sind in der Regel das richtige Mittel. Drei technische Punkte sind offen. Der erste betrifft DNSSEC. Ordnet das BSI einer Registry an, die Nameserver-Einträge einer signierten Domain zu ändern (§ 16a BSIG-E), liefern validierende Resolver keine Umleitung, sondern einen Fehler, solange niemand die Schlüsselkette anpasst. Dazu steht im Entwurf nichts.⁵⁴ Der zweite betrifft die Reichweite. Umleitungen über die Telekommunikationsanbieter erfassen nach der Begründung

⁴⁹Senatskanzlei Berlin (Fn. 21).

⁵⁰Fn. 10 und 38.

⁵¹r-tec IT Security, Abschlussbericht Security Incident Südwestfalen-IT, Version 1.1, 19. Januar 2024, S. 20 und 23; BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 10 (72 Kommunen).

⁵²Viasat, KA-SAT Network cyber attack overview, 30. März 2022; Enercon, Mitteilung vom 1. März 2022 (5.800 Anlagen); CyberScoop, Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault, 10. August 2023.

⁵³Gemeinsame Cybersecurity Advisory AA25-239A vom 27. August 2025, mitgezeichnet von BND, BfV und BSI.

⁵⁴BT-Drs. 21/6585, S. 13–14; DENIC, Nameserver Predelegation Check, technische Spezifikation, Abschnitt 3.1; ICANN, Guidance for Preparing Domain Name Orders, Seizures & Takedowns, 2012.

wegen „DNS over HTTPS“ „einen sehr großen Anteil des Botnetzverkehrs nicht“. Deshalb nimmt § 17 Abs. 2 Cloud- und CDN-Anbieter hinzu.⁵⁵ Für den DNS-Filter nach § 16 Abs. 7 gilt dieselbe Grenze. Er sieht nur Anfragen, die den Resolver des verpflichteten Anbieters erreichen, und er ist ein Angebot, das der Nutzer wählen muss. Der dritte betrifft geteilte Adressen. Hinter der IP-Adresse eines Cloud-Anbieters oder eines Mobilfunknetzes stehen viele Nutzer. Eine Sperre nach den fortschreibbaren Listen des § 16 Abs. 1 trifft sie alle. Geprüft werden muss das vor der Aufnahme in die Liste nicht.⁵⁶

Beim Eingriff in fremde Systeme fehlen Sicherungen. Der Richtervorbehalt gilt nur, wenn der Eingriff eine Datenerhebung ermöglicht und das System „als eigenes privat genutzt wird“ (§ 68e Abs. 1 und 2 BKAG-E); der gemietete Server, auf dem neben dem Steuerungsdienst eines Botnetzes die Buchhaltung eines Mittelständlers läuft, fällt nach dem Wortlaut nicht darunter. Veränderungen sind rückgängig zu machen, „soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht“ (§ 68d Abs. 3). Unklar ist, wer das vorab einschätzt und festhält. Beim BKA erstreckt er die besondere Protokollierung nur auf Eingriffe in private Systeme, bei der Bundespolizei auf alle.⁵⁷ Und als Zugangsweg nennt die Begründung ausdrücklich: „Möglich ist ferner die Ausnutzung vorhandener Schwachstellen.“⁵⁸ Ob Behörden eine Schwachstelle für sich behalten dürfen, wann sie sie dem Hersteller melden müssen und wer darüber entscheidet, regelt der Entwurf nicht. Eine Lücke, die eine Behörde offenhält, bleibt für alle offen, auch für die Angreifer, gegen die das Gesetz sich richtet. Für die Quellen-Telekommunikationsüberwachung hat das Bundesverfassungsgericht 2021 für unbekannte Sicherheitslücken „eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts“ verlangt. Bei der aktiven Cyberabwehr stellt sich derselbe Konflikt.⁵⁹ Nötig ist dieser Weg selten: „die meisten Maßnahmen der aktiven Cyberabwehr benötigen überhaupt keine Schwachstellen.“⁶⁰

Hinzu kommt das Zuordnungsproblem. Wer ein Angriffssystem im Netz findet, hat es lokalisiert. Wer den benennt, der dahintersteht, hat den Angriff attribuiert. Lokalisierung gelingt oft, Attribution ist deutlich schwieriger.⁶¹ Die Begründung hält die Identifizierung der beteiligten Systeme, also Lokalisierung, für „regelmäßig eindeutig möglich“, etwa anhand von IP-Adressen und Signaturen.⁶² Für eine Umleitung, die sich zurücknehmen lässt, mag das genügen. Für das Löschen von Daten auf einem Server im Ausland, woran die Begründung ausdrücklich denkt, genügt es nicht. Dort sollte auch feststehen, ob die Maßnahme nur einen Täter oder auch einen fremden Staat oder ein weiteres Opfer trifft. Das mag abhängig vom Fall vertretbar sein, und der Entwurf erlaubt auch Eingriffe, „wenn Dritte unvermeidbar betroffen werden“. Benachrichtigt wird allerdings nur der Inhaber des Systems, in das eingegriffen wurde.⁶³

Der Entwurf sieht keine Evaluierung vor. Die Auswirkungen seien „im Wesentlichen prognostizierbar“, und die bestehende Kontrolle durch Parlament, Aufsicht und Gerichte genüge. Der Normenkontrollrat lässt diese Gründe nicht gelten.⁶⁴ Die zwölf Beispiele sprechen gegen die Prognose. Wie lange eine Unterbrechung hält, wie oft sie Unbeteiligte trifft und wie schnell die Angreifer sich neu aufbauen, weiß man erst, wenn es jemand systematisch misst.

⁵⁵BT-Drs. 21/6585, Begründung S. 55–56.

⁵⁶BT-Drs. 21/6585, S. 13; zum Überblocking eco – Verband der Internetwirtschaft, Stellungnahme zum Referentenentwurf, 17. März 2026, S. 1–2.

⁵⁷BT-Drs. 21/6585, S. 20–22 (§§ 68d, 68e, 82 BKAG-E) und S. 10 (§ 85 BPolG-E), Begründung S. 68.

⁵⁸BT-Drs. 21/6585, S. 46.

⁵⁹BVerfG, Beschluss vom 8. Juni 2021, 1 BvR 2771/18, Leitsatz 2 b; die Verfassungsbeschwerde war unzulässig.

⁶⁰Impulspapier (Fn. 1), S. 5.

⁶¹Impulspapier (Fn. 1), S. 2.

⁶²BT-Drs. 21/6585, S. 44.

⁶³BT-Drs. 21/6585, S. 8–9 und 20–22 (§ 41a Abs. 3, § 78 BPolG-E; § 68d Abs. 4, § 74 BKAG-E), Begründung S. 60.

⁶⁴BT-Drs. 21/6585, S. 42–43; Stellungnahme des Nationalen Normenkontrollrats, ebenda S. 72.

4 Was andere Länder tun und was daraus folgt

Ähnliche Regelungen wie im vorliegenden Entwurf gibt es auch in anderen Ländern. Die Demokratien, die sie schon haben, fassen sie allerdings meist enger und kontrollieren sie strenger als der Entwurf.

Erstens entscheidet anderswo in der Regel eine unabhängige Stelle vorab über den Eingriff in ein fremdes System, unabhängig davon, ob es privat oder geschäftlich genutzt wird. In den USA beruhten die Operationen gegen Hafnium (2021), Snake und Qakbot (2023) und das KV-Botnetz (2024) jeweils auf einem richterlichen Beschluss. Australien verlangt seit 2021 für das Verändern von Daten den Beschluss eines Richters oder Tribunalmitglieds, die Niederlande im Strafverfahren die Ermächtigung des Untersuchungsrichters, Japan seit 2025 die vorherige Genehmigung einer unabhängigen Kommission.⁶⁵

Zweitens gibt es genauere Regelungen zur Abschätzung von Kollateralschäden und zum Auslandsbezug. Das australische Gesetz verpflichtet die genehmigende Stelle, die Folgen für rechtmäßige Nutzer des betroffenen Rechners abzuwägen. Japan lässt Eingriffe in Server, die nicht erkennbar im Inland stehen, nur durch die nationale Polizeibehörde zu und erst nach Abstimmung mit dem Außenminister.

Drittens gibt es Befristungen und Prüfaufträge. Australien hat die Befugnis auf zunächst fünf Jahre begrenzt und gesetzlich überprüfen lassen. Der Prüfer fand sie wirksam und selten genutzt („used sparingly“), das Genehmigungsverfahren aber untauglich. Das Parlament hat sie 2026 um drei Jahre verlängert und einer der beiden Behörden wieder entzogen.⁶⁶

5 Empfehlungen an den Gesetzgeber

1. **Das Lagebild zur gesetzlichen Aufgabe machen.** Das BSI sollte den Auftrag erhalten, fortlaufend zwei Lagebilder zu führen und zusammenzuführen: das der eigenen Angriffsfläche und das der Infrastruktur, die Angreifer aufbauen, mieten oder kapern. § 40 Abs. 3 Nr. 3 BSIG bietet dafür den Ansatz; er erfasst heute nur kritische Anlagen und NIS-2-Einrichtungen und nur deren eigene Sicherheit. BKA, Bundespolizei und Nachrichtendienste sollten verpflichtet werden, im Rahmen ihrer Aufgaben beizutragen, und die Länder sollten sich anschließen können.
2. **Die Befugnisse für die Datengrundlage klarstellen.** § 15 Abs. 1 BSIG sollte auch die Aufgaben nach § 3 Abs. 1 Satz 2 Nr. 2, 20 und 24 nennen, wie es der Regierungsentwurf zum NIS-2-Umsetzungsgesetz vorsah,⁶⁷ und ausdrücklich den wiederholten Abruf und Vergleich öffentlich erreichbarer Webinhalte samt einer Aufbewahrungsfrist regeln. § 8 BSIG sollte klarstellen bzw. festlegen, dass die automatisierte Suche mit neuen Indikatoren auch in Daten zulässig ist, die älter als drei Monate sind, pseudonymisiert und protokolliert, bevor eine Betroffenheit des Bundes feststeht. In die Registrierung nach § 33 BSIG gehören neben den IP-Adressbereichen die Domainnamen.
3. **Die Maßnahmen im Netz beschließen und technisch ergänzen:** durch eine Klausel in § 16a BSIG-E, die festlegt, wie bei einer signierten Domain mit DNSSEC verfahren wird; durch eine Prüfung vor der Listung einer IP-Adresse nach § 16 Abs. 1, die geteilte Adressen erkennt und

⁶⁵U.S. District Courts, 4:21-mj-755 (S.D. Tex.), 23-mj-0428 (E.D.N.Y.), 2:23-mj-4244 (C.D. Cal.), 4:23-mc-5530 (S.D. Tex.); Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Australien), s. 27KC; Art. 126nba Wetboek van Strafvordering; zu Japan Forschungsdienst des Unterhauses, RESEARCH BUREAU Ronkyu Nr. 22, Dezember 2025, S. 219 ff. (Gesetz vom 16. Mai 2025).

⁶⁶Identify and Disrupt Act 2021, s. 27KAA; J. Blight, Independent National Security Legislation Monitor, Bericht vom September 2025, S. i und Teil 2; Crimes and Other Legislation Amendment (Omnibus No. 1) Act 2026, Act No. 70 of 2026, Explanatory Memorandum.

⁶⁷BT-Drs. 21/1501, S. 29.

veraltete Einträge streicht; und durch eine Messung des BSI, welchen Anteil der Nutzer und der schädlichen Anfragen der Filter nach § 16 Abs. 7 erreicht, bevor die Pflicht in Kraft tritt. Klarstellen bzw. festlegen sollte das Gesetz, dass Anordnungen auch auf einzelne Konten, Schlüssel und Aufträge bei einem Cloud-Anbieter zielen können statt auf ganze Adressen.

4. **Den Richtervorbehalt an die Eingriffstiefe binden.** Er sollte für jeden Eingriff mit technischen Mitteln in ein fremdes System ohne Einwilligung des Berechtigten gelten (§ 68d BKAG-E, § 41a Abs. 1 Nr. 3 BPolG-E), im Eilfall mit Bestätigung binnen drei Tagen. Der Antrag sollte eine technische Einschätzung enthalten: was auf dem Zielsystem außer der Angriffsinfrastruktur läuft, worauf die Zuordnung beruht und welche Veränderungen sich zurücknehmen lassen. Das Gericht sollte einen unabhängigen technischen Sachverständigen hinzuziehen können; in Australien, das vergleichbare Befugnisse seit 2021 kennt, hält der unabhängige Prüfer das Anordnungsverfahren für „not fit for purpose“, auch weil den Entscheidern „independent technical advice“ fehlt.⁶⁸ Jeder dieser Eingriffe ist zu protokollieren, beim BKA wie bei der Bundespolizei, nicht nur der in private Systeme. Für § 68d BKAG-E hat auch der Bundesrat einen durchgehenden Richtervorbehalt verlangt.⁶⁹
5. **Den Umgang mit Schwachstellen regeln.** Dazu gehören feste Regeln für den Umgang mit neu gefundenen Schwachstellen, insbesondere ein Verfahren für die Entscheidung über das Zurückhalten unter Beteiligung des BSI und ein Bericht an den Bundestag. Eine vom Hersteller längst geschlossene Lücke auf einem ungepatchten Angriffsserver ist eine andere Sache.
6. **Dritte und den Auslandsbezug mitdenken.** Benachrichtigt werden sollte auch, wer von einem Eingriff mitbetroffen ist, etwa die übrigen Kunden eines geteilten Servers. Steht das Zielsystem im Ausland, sollte die Anordnung festhalten, wen die Maßnahme trifft, worauf diese Zuordnung beruht und wie sie sich völkerrechtlich rechtfertigt.
7. **Die Führung regeln.** Für zusammenhängende Operationen von BSI, BKA, Bundespolizei, Nachrichtendiensten, Ländern und Anbietern sollte das Gesetz sagen, wer führt und wie widersprüchliche Anordnungen entschieden werden. Das Benehmen allein leistet das nicht. Zur Führung gehören auch eine rund um die Uhr erreichbare Entscheidungsstelle und vorbereitete Schnittstellen zu den Anbietern, denn eine Anordnung, die nach dem Angriff eintrifft, schützt nur vor dem nächsten.
8. **Den Datenbestand des BSI schützen.** Für die Daten aus §§ 15 Abs. 6, 16, 16a, 17 und 31 BSIG-E sollte das Gesetz neben Zweckbindung und Löschfristen technische Mindestanforderungen nennen: verschlüsselte Übermittlung, getrennte Speicherung der Schwachstelleninformationen und eine unabhängige Prüfung.
9. **Zählen, befristen, evaluieren.** Eine jährliche öffentliche Statistik der Anordnungen je Befugnis für alle drei Behörden; eine Befristung der Eingriffsbefugnisse (§ 68d BKAG-E, § 41a Abs. 1 Nr. 3 BPolG-E) auf fünf Jahre; und vor der Verlängerung eine unabhängige Evaluierung, die soweit möglich die Zeit bis zur Erkennung und Wirkung, den vermiedenen Schaden, die Folgen für Unbeteiligte und den Wiederaufbau der Angreifer misst.

⁶⁸J. Blight, Independent National Security Legislation Monitor, Review of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021, September 2025, S. i.

⁶⁹BT-Drs. 21/7406, S. 2; die Bundesregierung lehnt ihn ab und sagt nur zu, die gerichtliche Zuständigkeit zu ergänzen, die in § 68e BKAG-E fehlt (S. 5).