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

Herrn MinRat Dr. Daniel Meltzian
Referat CI 1 – Grundsatz; Cyber- und Informationssicherheit
Bundesministerium des Innern
Alt-Moabit 140
10557 Berlin

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

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

Frankfurt am Main, 15.03.2026

Per E-Mail: CI1@bmi.bund.de

Schriftliche Stellungnahme zum

Referentenentwurf der Bundesregierung für ein „Gesetz zur Stärkung der Cybersicherheit“

Kritische Analyse der Befugnisse zur aktiven Cyberabwehr

Übersicht

I. Einführung: Zwischen Handlungsfähigkeit und Rechtsstaatlichkeit im Cyberraum

Die Bedrohungslage im Cyberraum hat sich in den vergangenen Jahren grundlegend verändert. Staatlich gelenkte Cyberangriffe, hochprofessionelle Ransomware-Kampagnen und hybride Bedrohungsszenarien, wie sie spätestens seit dem russischen Angriffskrieg gegen die Ukraine offenkundig geworden sind, stellen nicht nur die technische Resilienz kritischer Infrastrukturen, sondern auch die Säulen des bisherigen gefahrenabwehrrechtlichen Instrumentariums auf den Prüfstand. Es wäre daher verfehlt, den Referentenentwurf der Bundesregierung für ein „Gesetz zur Stärkung der Cybersicherheit“ pauschal abzulehnen. Im Gegenteil: Die Schaffung gesetzlicher Grundlagen für eine aktive Cyberabwehr ist im Grundsatz nicht nur vertretbar, sondern angesichts der sich qualitativ und quantitativ verschlechternden Bedrohungslage sachlich notwendig. Zahlreiche andere Staaten innerhalb und außerhalb der Europäischen Union – darunter Frankreich, die Niederlande, das Vereinigte Königreich und die Vereinigten Staaten – haben vergleichbare Befugnisse geschaffen oder befinden sich in entsprechenden Gesetzgebungsverfahren und politischen Diskussionen.

Dennoch darf das Gebot effektiver Gefahrenabwehr im digitalen Raum nicht dazu führen, dass rechtsstaatliche Grundsätze, die gerade in Zeiten erhöhter Bedrohung ihre schützende Funktion entfalten müssen, signifikant abgeschwächt werden. Mehr Cybersicherheit erfordert mehr staatliches Handeln, aber nicht weniger Rechtsstaatlichkeit. Der vorliegende Referentenentwurf weist in seiner derzeitigen Fassung erhebliche Defizite auf, die einer kritischen wissenschaftlich-analytischen Betrachtung bedürfen. Diese betreffen namentlich die technische Unbestimmtheit zentraler Regelungen, die ungelöste Attribuierungsproblematik, die verfahrensrechtlichen Sicherungsmechanismen, die Auswirkungen von getroffenen Maßnahmen auf unbeteiligte Dritte, die Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI), völkerrechtliche Implikationen sowie den staatlichen Umgang mit Sicherheitslücken und Zero-Day-Exploits. Die nachfolgende Stellungnahme unterzieht die zentralen Einzelvorschriften des Entwurfs einer differenzierten Analyse entlang dieser Leitlinien.

II. § 41a BPolG-E: Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik

Der neu vorgeschlagene § 41a BPolG-E räumt der Bundespolizei umfassende Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik ein. Das Instrumentarium umfasst die Untersagung des Betriebs informationstechnischer Systeme, die Umleitung, Einschränkung oder Unterbindung von Datenverkehr auch ohne Wissen der Betroffenen sowie die Erhebung, Löschung oder Veränderung von Daten durch Eingriff mit technischen Mitteln in ein informationstechnisches System. Damit wird ein Eingriffsarsenal geschaffen, das in seiner Tiefe und Reichweite erhebliche Parallelen zu nachrichtendienstlichen Befugnissen aufweist, ohne dass der Entwurf die damit verbundenen rechtsstaatlichen Implikationen insbesondere unter dem Gesichtspunkt des Trennungsgebots zwischen Polizei und Nachrichtendiensten hinreichend adressiert.

Besonders problematisch erscheint die in Absatz 4 enthaltene Regelung, wonach die Maßnahmen auch durchgeführt werden dürfen, wenn andere Personen „unvermeidbar“ betroffen werden. Zwar ist die Betroffenheit Dritter bei technisch komplexen Maßnahmen im Cyberraum kaum vollständig zu vermeiden, doch lässt die gegenwärtige Formulierung jede an sich erforderliche Näherbestimmung einer Verhältnismäßigkeitsprüfung vermissen. Es fehlt an einer Festlegung,

in welchem Umfang die Betroffenheit Dritter hinzunehmen ist und ab welcher Schwelle die Eingriffsintensität gegenüber Unbeteiligten das Maß des Vertretbaren überschreitet. Bei botnet-bezogenen Takedowns können potenziell Hunderttausende privater Endgeräte betroffen sein, deren Nutzer keine Verantwortung für den Angriff tragen.

Das in Absatz 10 vorgesehene Offenbarungsverbot, das es der Bundespolizei ermöglicht, u.a. dem Betreiber eines informationstechnischen Systems die Offenbarung der Maßnahme gegenüber den Betroffenen zu untersagen, verschärft die Problematik der verdeckten Durchführung weiterhin. Zwar ist nachvollziehbar, dass eine vorzeitige Offenbarung den Erfolg der Gefahrenabwehr oder Strafverfolgung gefährden kann; gleichwohl fehlt es an einer zeitlichen Begrenzung des Offenbarungsverbots sowie an einer unabhängigen Kontrolle seiner Anordnung und Fortdauer. Die Bußgeldbewehrung eines Verstoßes gegen das Offenbarungsverbot mit bis zu 20 Millionen Euro erscheint überdies mit Blick auf die damit einhergehende Einschüchterungswirkung gegenüber kooperierenden Unternehmen als unverhältnismäßig hoch.

In verfahrensrechtlicher Hinsicht ist festzuhalten, dass der Richtervorbehalt nach Absatz 6 lediglich für Maßnahmen vorgesehen ist, die in private informationstechnische Systeme eingreifen und eine Datenerhebung ermöglichen. Maßnahmen nach Absatz 2 Nummer 1 (Betriebsuntersagung) und Nummer 2 (Umleitung und Unterbindung von Datenverkehr) unterliegen hingegen keinem vergleichbaren Schutz, obwohl auch sie eine erhebliche Grundrechtsrelevanz aufweisen können. Die bloße Einordnung als „keine Überwachungsmaßnahmen“ in der Entwurfsbegründung ist rechtsdogmatisch nicht überzeugend, da auch die Umleitung und Aufzeichnung von Datenverkehr eine Kenntnisnahme potenziell persönlichkeitsrelevanter Kommunikationsinhalte ermöglichen kann. Ob eine Kenntnisnahme tatsächlich erfolgt oder für Ermittlungen relevant ist, ist juristisch nicht entscheidend, soweit allein die technische Möglichkeit hierzu besteht bzw. geschaffen wird.

III. § 16a und § 17 Abs. 2 BSIG-E: Anordnungsbefugnisse des BSI gegenüber Top Level Domain Registries und Registraren

Die neu einzufügenden §§ 16a und 17 Abs. 2 BSIG-E erweitern die Anordnungsbefugnisse des Bundesamtes für Sicherheit in der Informationstechnik gegenüber Top Level Domain Name Registries, Registraren und weiteren Diensteanbietern erheblich. Das BSI kann künftig anordnen, dass Nameserver-Einträge geändert oder ergänzt werden, und nach § 17 Abs. 2 BSIG-E auch die Umleitung oder Unterbindung von Datenverkehr veranlassen. Der Wegfall der aufschiebenden Wirkung von Widerspruch und Anfechtungsklage in § 16a Abs. 1 Satz 2 unterstreicht die Dringlichkeit, mit der der Gesetzgeber diese Maßnahmen zu versehen beabsichtigt.

Aus der Perspektive der Rolle des BSI als unabhängige, technisch ausgerichtete Fachbehörde zur gesamtgesellschaftlichen Stärkung operativer Cybersicherheit und digitaler Resilienz wirft die zunehmende Einbindung in operative Cyberabwehrmaßnahmen grundsätzliche Fragen auf. Das BSI wurde historisch als technische Fachbehörde konzipiert, die vorrangig beratend und unterstützend tätig wird. Die Ausweitung operativer Befugnisse, insbesondere die Möglichkeit zur Anordnung von Nameserver-Umleitungen und die damit verbundene Datenverarbeitung, rückt das BSI in eine Funktion, die zunehmend gefahrenabwehrrechtlichen Charakter trägt und seiner bisherigen Rolle kaum gerecht wird. Diese Funktionsverschiebung birgt die Gefahr, dass das Vertrauen der Wirtschaft und der Öffentlichkeit in das BSI als neutrale und unabhängige Instanz untergraben wird – ein Vertrauen, das für die Zusammenarbeit mit Unternehmen, insbesondere bei der Meldung von Sicherheitsvorfällen nach der NIS-2-Richtlinie, von elementarer Bedeutung ist. Diese Fragestellungen und Probleme wurden bereits in der vergangenen Legislaturperiode

von den Expert:innen in der „AG BSI“ umfassend dargestellt und in den bundespolitischen Diskurs eingebracht, zu denen auch der Verfasser dieser Stellungnahme zählt. Die in § 16a Abs. 2 BSIG-E vorgesehene Informationspflicht gegenüber der Bundesdatenschutzbeauftragten lediglich in Form eines jährlichen aggregierten Berichts über die Gesamtzahl der Nameserver-Umleitungen stellt angesichts der Eingriffsintensität ein unzureichendes Kontrollniveau für diese Maßnahmen und ihre grundrechtliche Relevanz dar.

Ferner adressiert der Entwurf die Frage der digitalen Souveränität im Hinblick auf die technologischen Mittel für die aktive Cyberabwehr nicht. Weder in den Gesetzesnormen noch in der Begründung findet sich eine belastbare Aussage dazu, welche technischen Werkzeuge und Plattformen für die Durchführung der Maßnahmen eingesetzt werden sollen und ob diese aus europäischer Entwicklung stammen oder von technologisch unsouveränen Drittstaatanbietern bezogen werden. Gerade bei der Umleitung von Datenverkehr und dem Betrieb von Sinkholes sind die eingesetzten Infrastrukturen sicherheitskritisch, da ein Zugriff Dritter auf die umgeleiteten Daten nicht ausgeschlossen werden kann, wenn die zugrundeliegende Technologie nicht vertrauenswürdig kontrollierbar ist.

IV. § 3a BKAG-E: Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik bei internationaler Zusammenarbeit oder außen- und sicherheitspolitischer Bedeutung

Die Schaffung des § 3a BKAG-E begründet eine neue Aufgabe des Bundeskriminalamtes für die Abwehr von Cybergefahren bei internationaler Zusammenarbeit oder außen- und sicherheitspolitischer Bedeutung. Die Vorschrift definiert den Anwendungsbereich über den Verweis auf die §§ 202a, 202b, 202c, 202d, 263a, 303a und 303b StGB und differenziert zwischen schwerwiegenden Angriffen im Kontext internationaler Kooperation und Angriffen von außen- und sicherheitspolitischer Bedeutung.

Obwohl die Entwurfsbegründung betont, dass es sich nicht um eine allgemeine Zuständigkeit für die polizeiliche Gefahrenabwehr im Cyberraum handele, sind die verwendeten Tatbestandsmerkmale auslegungsfähig und in ihrer Abgrenzung zu den Zuständigkeiten der Landespolizeien nicht hinreichend trennscharf. Das Kriterium der „außen- und sicherheitspolitischen Bedeutung“ in Absatz 1 Nummer 2 ermöglicht eine extensive Interpretation, da nahezu jeder größere Cyberangriff auf kritische Infrastrukturen auch außenpolitische Implikationen haben kann. Die behördlichen Zuständigkeiten im Notfall bleiben damit unklar; insbesondere fehlt es an einer geregelten Koordination zwischen BKA, Bundespolizei, BSI und den Landespolizeibehörden für den Fall, dass mehrere Behörden gleichzeitig zuständig sind oder zu sein beanspruchen. Überdies findet sich kein Koordinationsmechanismus zur Abgrenzung der Zuständigkeit des BND bei Auslandssachverhalten.

Ebenfalls wirft der skizzierte Vorstoß erhebliche völkerrechtliche Fragen auf, die der Entwurf nicht angemessen behandelt. Maßnahmen der aktiven Cyberabwehr, die IT-Systeme im Ausland betreffen – wie etwa das Verändern oder Löschen von Daten auf ausländischen Servern –, berühren im Zweifelsfall auch die Souveränität anderer Staaten – zumindest lässt sich dies nicht ohne Weiteres im Vorfeld ausschließen. Die völkerrechtliche Debatte zur Effekt-Äquivalenz von Cyberoperationen im Vergleich zu konventionellen militärischen Operationen ist keineswegs abgeschlossen. Der vorgelegte Gesetzentwurf enthält keine Regelungen zur Abgrenzung gegenüber dem Kommando Cyber- und Informationsraum der Bundeswehr, obwohl gerade bei Angriffen mit außen- und sicherheitspolitischer Dimension die Grenze zwischen polizeilicher Gefahrenabwehr und militärischer Cyberverteidigung verschwimmen kann und hier

verfassungsrechtlich deutlich höhere Hürden anzusetzen wären. Auch das Tallinn Manual 2.0 und die Verhandlungen im Rahmen des UN Open-Ended Working Group-Prozesses zeigen, dass die völkerrechtlichen Standards für staatliche Cyberoperationen noch in der Entwicklung sind und eine vorschnelle Schaffung weitreichender Eingriffsbefugnisse ohne begleitende völkerrechtliche Einordnung rechtlich nachhaltig problematisch sein kann.

V. §§ 62b bis 62g BKAG-E: Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik

1) § 62b BKAG-E: Generalklausel und Befugnisverknüpfung („Befugnisse“)

§ 62b BKAG-E schafft eine polizeiliche Generalklausel für die Cyberabwehr und verknüpft die neuen Befugnisse mit den bereits bestehenden Instrumenten des BKAG, darunter Observation, Telekommunikationsüberwachung, Durchsuchung und Sicherstellung. Die Vorschrift setzt dabei lediglich das Vorliegen einer konkreten Gefahr voraus und verweist zur Gefahrendefinition auf die Straftatbestände der §§ 202a ff. und 303a f. StGB. Damit wird ein weites Eingriffsfeld eröffnet, das in der Kombination mit den spezifischen Befugnissen der §§ 62c bis 62g zu einem kumulativ erheblichen Grundrechtseingriff führen kann. Das Fehlen einer qualifizierten Gefahrenschwelle für die Anwendung der Generalklausel selbst – abgesehen von den besonderen Anforderungen des § 62f für Eingriffe in private Systeme – ist angesichts der Eingriffstiefe der verfügbaren Maßnahmen rechtsstaatlich bedenklich.

2) § 62c BKAG-E: Untersagung des Betriebs informationstechnischer Systeme

Die Befugnis zur Untersagung des Betriebs informationstechnischer Systeme nach § 62c BKAG-E ist zumindest konzeptionell als niedrigschwelligstes Instrument der Cyberabwehr einzuordnen. Gleichwohl kann die Untersagung des Betriebs eines Servers oder einer Infrastruktur weitreichende Folgen für Dritte haben, die denselben Server nutzen, ohne an dem Angriff beteiligt zu sein. Der Entwurf enthält keine spezifischen Vorgaben für eine Folgenabschätzung oder eine Abwägung der Auswirkungen auf unbeteiligte Nutzer, die denselben Hosting-Anbieter oder dieselbe Cloud-Infrastruktur verwenden. Hier besteht deshalb dringender verfahrensrechtlicher Nachbesserungs- und Konkretisierungsbedarf.

3) § 62d BKAG-E: Einschränkung, Unterbindung und Umleitung von Datenverkehr

Die in § 62d BKAG-E vorgesehene Befugnis zur Einschränkung, Unterbindung und Umleitung von Datenverkehr auch ohne Wissen der Betroffenen stellt einen erheblichen Eingriff in die Vertraulichkeit der Kommunikation und in das Fernmeldegeheimnis dar. Die Entwurfsbegründung verweist zwar auf die Erforderlichkeit zur Analyse von Angriffsmustern und zur Aufklärung der Ursprünge von Cyberangriffen, doch fehlt es an konkreten technischen Umsetzungsmaßstäben. Der Entwurf beschreibt zwar in der juristischen Theorie, was geschehen soll – die Umleitung auf ein Sinkhole, das Filtern von Metadaten anhand individueller Signaturen –, ohne jedoch zu klären, welche technischen Standards bei der Implementierung einzuhalten sind, wie die Integrität umgeleiteter Daten gewährleistet wird und welche Mindestanforderungen an die Protokollierung der erfassten Daten bestehen, um die Sachdienlichkeit der angeordneten Maßnahmen gewährleisten zu können. Die Verpflichtung, sich gemäß Absatz 3 bei einer Umleitung von Datenverkehr mit dem BSI ins Benehmen zu setzen, ist zwar ein erster Schritt, bleibt aber hinter einer

tatsächlichen Freigabepflicht und detaillierten fachlichen Abstimmung aus Sicht der Cybersecurity zurück.

4) § 62e BKAG-E: Erheben, Löschen und Verändern von Daten in informationstechnischen Systemen

Die weitreichendste und zugleich mit Abstand problematischste Befugnis des gesamten Entwurfs findet sich in § 62e BKAG-E, der das Bundeskriminalamt ermächtigt, Daten eines informationstechnischen Systems auch durch Eingriff mit technischen Mitteln ohne Wissen des Betroffenen zu erheben, zu löschen oder zu verändern. Die Entwurfsbegründung erläutert hierzu Szenarien wie die Übernahme von Command-and-Control-Servern, das Senden von Deinstallationsbefehlen an infizierte Bots und die Veränderung angreiferseitiger Skripte. In der technischen Praxis sind diese Maßnahmen von erheblicher Komplexität und Fehleranfälligkeit. Der Entwurf lässt die zentrale Frage unbeantwortet, nach welchen technischen Maßstäben die eingesetzten Werkzeuge zu entwickeln, zu testen und freizugeben sind. Es fehlen Regelungen zur Qualitätssicherung, zur unabhängigen technischen Prüfung der eingesetzten Software und technischen Verfahren sowie zur Haftung und rechtlichen Verantwortlichkeit bei fehlerhaften Eingriffen, die zu Schäden an den betroffenen Systemen führen.

Die Formulierung in Absatz 2, wonach vorgenommene Veränderungen bei Beendigung der Maßnahme rückgängig zu machen sind, „soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht“, enthält einen doppelten Vorbehalt, der die Pflicht zur Wiederherstellung des ursprünglichen Zustands weitgehend relativiert, ohne dies an belastbare Kriterien anzuknüpfen. In Absatz 3 wird zudem festgelegt, dass die Maßnahmen auch durchgeführt werden dürfen, wenn andere Personen unvermeidbar betroffen werden, ohne dies weitergehend zu konkretisieren. In Verbindung mit der fehlenden qualitativen und quantitativen Begrenzung dieser Drittbetroffenheit ergibt sich in der Gesamtschau der Befugnisgrundlage ein erhebliches Defizit, das vor dem Hintergrund der Verhältnismäßigkeitsanforderungen des Bundesverfassungsgerichts kaum haltbar erscheint und deshalb dringender Überarbeitung bedarf.

5) § 62f BKAG-E: Besondere Bestimmungen für Eingriffe in private Systeme

§ 62f BKAG-E normiert besondere Anforderungen für Eingriffe in private informationstechnische Systeme und sieht hierfür eine qualifizierte Gefahrenschwelle – dringende Gefahren für enumerativ aufgezählte Schutzgüter – sowie einen Richtervorbehalt vor. Dieser Regelungsansatz trägt den Anforderungen des Bundesverfassungsgerichts an den Schutz des IT-Grundrechts im Grundsatz Rechnung, weist jedoch im Detail einige Schwächen auf.

- Erstens ermöglicht die Eilfallregelung in Absatz 2 die Anordnung durch die Präsidentin oder den Präsidenten des BKA oder deren Vertretung, wobei die gerichtliche Bestätigung innerhalb von drei Tagen nachzuholen ist. Diese Frist erscheint angesichts der Eingriffsintensität – es handelt sich um den verdeckten Zugriff auf private IT-Systeme – als zu lang bemessen und sollte daher auf maximal 24 Stunden verkürzt werden. Die Möglichkeit, die Antrags- und Anordnungsbefugnisse auf Bedienstete mit Befähigung zum Richteramt zu delegieren, verwischt zudem die Verantwortungsstrukturen.
- Zweitens lässt die Legaldefinition des privaten informationstechnischen Systems in Absatz 3 Fragen offen. Die Negativabgrenzung, wonach ein System nicht privat ist, „wenn es im Wesentlichen für die Durchführung von Angriffen auf die Sicherheit in der Informationstechnik betrieben wird“, verschiebt die Beweislast faktisch zulasten des Betroffenen und ermöglicht es der Behörde, den besonderen Schutz privater Systeme zu umgehen, indem sie das System aufgrund von Indizien als nicht privat einordnet und dem

Betroffenen, der unter Umständen nicht einmal Kenntnis von dem Eingriff erlangt hat, die inhaltlich erhebliche Darlegungslast überträgt. Dies wirft die Frage auf, ob die Eingriffshürden für private Systeme nicht deutlich höher anzusetzen wären, insbesondere da auch kompromittierte Opfersysteme – die nach wie vor privat sind – als Angriffsinfrastruktur missbraucht werden können.

- Drittens fehlt es an einer verbindlichen gesetzlichen Bestimmung der maximalen Dauer von Eingriffen in private Systeme. Der Entwurf verlangt lediglich die Angabe eines Endzeitpunkts in der Anordnung, ohne eine Höchstdauer festzulegen. Dies steht im Widerspruch zu den verfassungsgerichtlichen Anforderungen an die zeitliche Begrenzung heimlicher Grundrechtseingriffe, die Kernbereichsrelevanz entfalten können.

6) § 62g BKAG-E: Offenbarungsverbot

Das Offenbarungsverbot nach § 62g BKAG-E ermöglicht es dem BKA, Betreibern und Diensteanbietern die Offenbarung der Maßnahme gegenüber den Betroffenen zu untersagen. Die Regelung enthält keine zeitliche Befristung, sondern lediglich die funktionale Grenze, dass die Offenbarung Zwecken der Gefahrenabwehr oder Strafverfolgung entgegenstehen muss. In Verbindung mit der Bußgeldbewehrung nach § 87a BKAG-E in Höhe von bis zu 20 Millionen Euro für Verstöße gegen das Offenbarungsverbot entsteht ein erheblicher Druck auf kooperationspflichtige Unternehmen. Aus rechtsstaatlicher Perspektive ist die Abwesenheit einer unabhängigen, richterlichen Überprüfung des Offenbarungsverbots ebenso zu kritisieren wie die fehlende automatische Befristung der Geheimhaltungspflicht.

VI. Technische Unbestimmtheit und Attribuierungsproblematik

Über die Beurteilung der konkreten Vorschriften hinausgehend liegt ein zentrales Defizit des Entwurfs in der systematischen Nichtbehandlung der Attribuierungsproblematik. Die Zurechnung eines Cyberangriffs zu einem bestimmten Akteur – sei es ein Staat, eine kriminelle Organisation oder ein einzelner Täter – ist technisch nach wie vor eine der größten Herausforderungen der internationalen Cybersicherheit. Die im Entwurf vorgesehenen Maßnahmen, insbesondere das Eindringen in fremde IT-Systeme und das Verändern oder Löschen von Daten, setzen voraus, dass das Ziel der Maßnahme korrekt identifiziert wurde. Eine fehlerhafte Attribuierung kann dazu führen, dass Maßnahmen gegen unbeteiligte IT-Systeme gerichtet werden, die lediglich als Proxy-Server oder Umleitungsinfrastruktur missbraucht werden. Der Entwurf enthält keine Regelungen, die eine Mindestverlässlichkeit der Attribuierung vor Durchführung aktiver Maßnahmen sicherstellen – etwa durch ein Mehraugenprinzip, durch eine obligatorische technische Bewertung seitens des BSI oder durch die Festlegung von Zuverlässigkeitsstandards für die Zurechnung.

Hinzu tritt das grundlegende Problem der „false flag"-Operationen, bei denen staatliche Akteure ihre Angriffe gezielt so gestalten, dass sie einem anderen Akteur zugerechnet werden. Die technische Realität zeigt, dass IP-Adressen gefälscht, Schadsoftware-Signaturen imitiert und Infrastrukturen über mehrere Länder hinweg kaskadiert werden können. Eine Maßnahme der aktiven Cyberabwehr auf der Grundlage fehlerhafter Attribuierung kann nicht nur die Rechte unschuldiger Dritter verletzen, sondern im völkerrechtlichen Kontext auch diplomatische Krisen auslösen.

VII. Trennungsprinzip und verfassungsrechtliche Dimension

Der Entwurf wirft erhebliche Fragen im Hinblick auf das verfassungsrechtlich zu gewährleistende Trennungsprinzip zwischen Polizei und Nachrichtendiensten auf. Die in § 62e BKAG-E sowie in § 41a BPolG-E vorgesehenen Befugnisse zum verdeckten Eingriff in informationstechnische Systeme ohne Wissen des Betroffenen, zur heimlichen Datenerhebung und zur Manipulation fremder IT-Infrastruktur entsprechen in ihrem operativen Charakter den Tätigkeitsfeldern der Nachrichtendienste. Das Trennungsprinzip, das in Deutschland zwischen polizeilichen und nachrichtendienstlichen Befugnissen unterscheidet, soll sicherstellen, dass nicht dieselbe Behörde zugleich nachrichtendienstlich aufklärt und polizeilich eingreift. Die Begründung des Entwurfs betont zwar, dass es sich um Gefahrenabwehrmaßnahmen und nicht um Überwachungsmaßnahmen handele, doch ist diese Unterscheidung in der operativen Praxis der Cyberabwehr jenseits solcher rein deklaratorischen Formulierungen nur schwer aufrechtzuerhalten. Das Eindringen in ein IT-System, das Auslesen von Konfigurationsdaten und die Analyse einer Angriffsinfrastruktur generieren zwangsläufig auch nachrichtendienstlich relevante Erkenntnisse. Ohne klare gesetzliche Regelungen zur informationellen Trennung und zur Verwendungsbeschränkung der gewonnenen Daten droht eine faktische Erosion des Trennungsprinzips.

VIII. Umgang mit Schwachstellen und Zero-Day-Exploits

Die rechtspolitische Debatte der vergangenen Jahre zu den Themen Hackback, digitale Gegenmaßnahmen und aktive Cyberabwehr hat die Frage des staatlichen Umgangs mit Sicherheitslücken und Zero-Day-Exploits als einen der zentralen Kritikpunkte herausgearbeitet. Wenn staatliche Behörden Schwachstellen in IT-Systemen bewusst offenhalten, um sie für aktive Abwehrmaßnahmen nutzen zu können, stehen sie in einem diametralen Zielkonflikt mit dem verfassungsrechtlichen Auftrag zur IT-Sicherheitsvorsorge, der gerade die schnellstmögliche Schließung bekannter Schwachstellen gebietet. Der Entwurf enthält hierzu keinerlei Regelung, noch wird die Problematik ansatzweise adressiert. Weder wird ein Vulnerability Equities Process nach dem Vorbild anderer Staaten vorgesehen, der eine strukturierte Abwägung zwischen dem Nutzen des Offenhaltens und dem Risiko einer Ausnutzung durch Dritte ermöglicht, noch werden Vorgaben zur Beschaffung von Schwachstellenwissen gemacht. Insoweit steht die fachliche Debatte hierzulande noch ganz am Anfang. Die Frage, ob Behörden Zero-Day-Exploits auf dem sogenannten „grauen Markt“ erwerben dürfen – einem Markt, auf dem auch autoritäre Regime und kriminelle Akteure als Käufer auftreten –, wird im Entwurf vollständig ausgespart. Ein Gesetz, das staatlichen Behörden Befugnisse zum Eindringen in fremde IT-Systeme einräumt, ohne gleichzeitig den Umgang mit den dafür erforderlichen Schwachstellen zu regeln, weist eine strukturelle Lücke auf, die aus sicherheitspolitischer wie aus grundrechtlicher Perspektive nicht hinnehmbar ist.

IX. Defizite bei Freigabe-, Protokoll- und Kontrollpflichten

Die verfahrensrechtlichen Sicherungsmechanismen des Entwurfs bleiben insgesamt hinter dem zurück, was angesichts der Eingriffstiefe der vorgesehenen Maßnahmen verfassungsrechtlich geboten wäre. Die Protokollierungspflichten beschränken sich bei § 41a BPolG-E auf Eingriffe in private Systeme; für die quantitativ weitaus häufigeren und potenziell ebenso grundrechtsrelevanten Maßnahmen nach Absatz 2 Nummern 1 und 2 fehlt eine vergleichbare Pflicht. Im BKAG verweisen die Berichtspflichten auf die bestehenden Kontrollregelungen, ohne spezifische Berichtsinhalte oder Berichtsintervalle für Cyberabwehrmaßnahmen festzulegen.

Auch die interne Freigabestruktur weist Defizite auf. Der Entwurf sieht für Maßnahmen nach § 62e BKAG-E, die nicht in private Systeme eingreifen, weder einen Richtervorbehalt noch eine anderweitige unabhängige Kontrolle vor. Das Eindringen in Server, die als Angriffsinfrastruktur dienen, das Löschen von Schadsoftware auf Drittgeräten oder das Verändern von Routing-Konfigurationen kann erhebliche Kollateralschäden verursachen und bedarf deshalb einer gestuften Freigabestruktur, die über die bloße Anordnungskompetenz der Behördenleitung hinausgeht. Ein Modell, das für Maßnahmen mit hohem Eskalationspotenzial eine ressortübergreifende Prüfung – etwa unter Einbeziehung des Bundesministeriums des Innern und des BSI – vorsieht, wäre der Komplexität und Tragweite der Maßnahmen angemessener.

Die Entwurfsbegründung stellt ausdrücklich fest, dass weder eine Befristung noch eine Evaluierung der Regelungen vorgesehen sind. Dies ist angesichts der Neuartigkeit der Befugnisse und der rasanten technologischen Entwicklung im Cyberbereich bemerkenswert. Andere sicherheitsrechtliche Gesetzgebungsvorhaben mit vergleichbarer Eingriffstiefe im digitalen Raum wurden mit Evaluationsklauseln versehen. Das Fehlen einer solchen Klausel erschwert die parlamentarische und öffentliche Überprüfung der tatsächlichen Auswirkungen der neuen Befugnisse und ihrer verhältnismäßigen Anwendung in der Praxis.

X. Schlussbetrachtung: Mehr digitale Sicherheit erfordert nicht automatisch weniger Recht

Der Referentenentwurf für ein „Gesetz zur Stärkung der Cybersicherheit“ adressiert ein reales und dringendes Problem: Die Bedrohungslage im Cyberraum hat sich in einer Weise entwickelt, die ein Festhalten an rein defensiven Strategien zunehmend unzureichend erscheinen lässt. Die Schaffung gesetzlicher Grundlagen für eine aktive Cyberabwehr, die auch Maßnahmen jenseits der eigenen Netzwerkgrenzen ermöglicht, ist im Grundsatz richtig und notwendig. Deutschland darf den Anschluss an die internationalen Entwicklungen nicht verlieren und muss seine Handlungsfähigkeit im digitalen Raum stärken.

Zugleich zeigt die vorliegende Stellungnahme, dass der Entwurf in seiner gegenwärtigen Fassung erhebliche rechtsstaatliche Defizite aufweist, die vor einer Verabschiedung dringend behoben werden müssen. Die technische Unbestimmtheit zentraler Regelungen, die nicht gelöste Attribuierungsproblematik, die unzureichenden verfahrensrechtlichen Sicherungsmechanismen, die problematische Betroffenheit dritter Personen, die ungeklärte Frage der digitalen Souveränität bei den eingesetzten Technologien, die geheime Durchführung der Maßnahmen, die Verhältnismäßigkeitsbedenken, die Funktionsverschiebung des BSI, die offenen völkerrechtlichen Fragen, die Spannungen mit Blick auf das Trennungsprinzip, die fehlenden Eingriffshürden bei nicht-privaten Systemen und das gänzliche Fehlen einer Regelung zum Umgang mit Schwachstellen und Zero-Day-Exploits – all diese Punkte zeigen einen erheblichen Nachbesserungsbedarf auf.

Ein Gesetz, das die staatliche Handlungsfähigkeit im Cyberraum stärken soll, muss sich an den höchsten rechtsstaatlichen Maßstäben messen lassen. Dies erfordert die Einführung eines strukturierten Vulnerability Equities Process, die Verankerung technischer Mindeststandards für die eingesetzten Werkzeuge, die Schaffung eines gestuften Freigabe- und Kontrollsystems, die Aufnahme von Evaluationsklauseln und ggf. gesetzlichen Befristungen, die Klärung der behördlichen Zuständigkeiten und ihrer Koordination im Notfall, die Festlegung höherer Schwellen für Eingriffe in private Systeme, die Normierung zeitlicher Grenzen für verdeckte Maßnahmen und Offenbarungsverbote sowie eine klare Abgrenzung zu nachrichtendienstlichen und militärischen Befugnissen.

Im Ergebnis lässt sich festhalten: Die Cybersicherheit benötigt durchaus mehr staatliches Handeln als in der Vergangenheit. Doch dieses Mehr an Handlungsfähigkeit darf nicht zwangsläufig mit einem Weniger an Rechtsstaatlichkeit einhergehen. Gerade in einem Bereich, der durch technische Komplexität, geringe öffentliche Sichtbarkeit und hohe Fehleranfälligkeit gekennzeichnet ist, müssen die rechtsstaatlichen Sicherungen besonders robust ausgestaltet sein. Der Gesetzgeber hat es in der Hand, ein Gesetz zu schaffen, das sowohl der Bedrohungslage angemessen als auch des Rechtsstaats würdig ist. Der vorliegende Entwurf erfüllt diesen Anspruch in seiner derzeitigen Fassung noch nicht.