AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

# Stellungnahme zum Ref-E des Bundesministeriums des Innern (BMI) für ein Gesetz zur Stärkung der Cybersicherheit

## im Rahmen der Verbändebeteiligung

Version 1.0 – zuletzt editiert am 12.03.2026

# Inhaltsverzeichnis

# 1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 23 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen.
Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

# 2 Vorwort

Der vorliegende Referentenentwurf enthält Regelungen sehr unterschiedlicher Qualität. Wir differenzieren deshalb in unserer Bewertung ausdrücklich zwischen Maßnahmen, die wir als sachgerecht und verhältnismäßig unterstützen, und solchen, die wir ablehnen, weil sie die Versorgungssicherheit der Bevölkerung und die Resilienz kritischer Infrastrukturen gefährden.

Unsere Analyse folgt der Leitfrage: Erhöhen die vorgesehenen Maßnahmen objektiv die Sicherheit kritischer Infrastrukturen und die Versorgungssicherheit der Bevölkerung, oder erzeugen sie neue, strukturell nicht beherrschbare Risiken?

# 3 Stellungnahme

## 3.1 sinnvolle Maßnahmen

Der Entwurf enthält im Bereich des BSI-Gesetzes mehrere Regelungen, die wir als grundsätzlich zielführend bewerten. Unsere Unterstützung ist dabei mit konkreten Nachbesserungsforderungen verbunden.

### 3.1.1 Schadprogramm-Erkennung - Änderung § 8 BSIG

Die Verbesserungen für den Betrieb des Schadprogramm-Erkennungssystems zum Schutz der Kommunikationstechnik des Bundes sind sachgerecht. Der Entwurf ändert § 8 Abs. 2 BSIG dahingehend, dass Protokolldaten länger gespeichert werden dürfen.

Die Schadprogrammerkennung operiert ohne aktive Eingriffsbefugnisse in fremde Systeme und ist rein auf Detektion ausgerichtet. Die Ausweitung der Speicherfrist ist operativ nachvollziehbar, da Angriffskampagnen regelmäßig über Monate unentdeckt laufen. Die parlamentarische Berichtspflicht ist dabei auf die Anwendung dieser erweiterten Speicherfristen zu erstrecken.

### 3.1.2 Erweiterung der BSI-Befugnis / Früherkennungsfälle – Änderung § 11 BSIG

Der Entwurf ändert § 11 Abs. 1 BSIG dahingehend, dass das BSI nicht mehr nur bei eingetretenen Beeinträchtigungen auf Ersuchen tätig werden darf, sondern bereits „bei Vorliegen von Anhaltspunkten für eine solche Beeinträchtigung“. Die Gesetzesbegründung erläutert, dass damit auch Fälle des sogenannten Prepositionings – also des vorbereitenden Eindringens von Angreifern vor Schadenseintritt – erfasst werden sollen, und bezeichnet diesen Vorgang als „Threat Hunting“. Im Normtext selbst tauchen diese Begriffe nicht auf.

Die bisherige Rechtslage, die einen eingetretenen Schaden als Voraussetzung für den BSI-Unterstützungseinsatz verlangte, war operativ suboptimal. Prepositioning ist eine gefährliche Angriffsphase: Angreifer etablieren in dieser Phase Persistenz, gewinnen Lageinformationen und bereiten ihre Wirkmöglichkeiten vor, ohne dass ein beobachtbarer Schaden eingetreten ist. Die Anforderung, dass ein Schaden bereits eingetreten sein muss, bevor das BSI unterstützen darf, ist daher nicht mehr zeitgemäß.

Die Regelung ist aus unserer Sicht tragfähig, weil der Wortlaut das Ersuchen der betroffenen Einrichtung als Voraussetzung formuliert.

### 3.1.3 Anordnungsbefugnisse gegenüber DNS-Anbietern – §§ 16a, 17 Abs. 2 BSIG-neu

Der Entwurf fügt § 16a BSIG-neu ein und ergänzt § 17 BSIG um einen neuen Absatz 2. Die Befugnisse ermöglichen dem BSI, gegenüber Top Level Domain Name Registries, Domain-Name-Registry-Dienstleistern und weiteren Diensteanbietern Nameserver-Änderungen und Umleitungen anzuordnen.

DNS-Infrastruktur spielt bei der Verbreitung von Schadsoftware und beim Betrieb von Command-and-Control-Infrastruktur eine zentrale Rolle. Die Befugnis zur raschen behördlichen Reaktion auf maliziöse DNS-Infrastruktur entspricht internationalem Standard. Positiv ist, dass § 16a Abs. 2 BSIG-neu eine Pflicht zur jährlichen Unterrichtung des Bundesdatenschutzbeauftragten vorsieht.

Kritisch ist, dass der Adressatenkreis in § 17 Abs. 2 BSIG-neu durch Verweis auf § 2 Nummern 4, 5, 25, 26 und 35 BSIG definiert wird, ohne im Entwurf selbst eine lesbare Aufzählung der erfassten Anbietertypen zu enthalten. Für Betreiber und Öffentlichkeit ist damit nicht unmittelbar erkennbar, welche Akteure verpflichtet werden.

Dies ist aus Sicht der Rechtsklarheit mangelhaft. Der Gesetzgeber sollte eine verständliche Beschreibung des Verpflichtetenkreises in die Gesetzestexte aufnehmen oder als Anlage beifügen. Ebenso fehlt eine explizite Verpflichtung zur Dokumentation des Umfangs und der Begründung einzelner Anordnungen gegenüber dem Deutschen Bundestag – die allgemeine Unterrichtung des Datenschutzbeauftragten genügt nicht.

### 3.1.4 Informationspflichten der TK- und digitalen Diensteanbieter – § 15 Abs. 6 BSIG-neu

Die Erweiterung der Informationspflichten auf digitale Diensteanbieter ist sachgerecht und entspricht dem Modell der kooperativen Cybersicherheit. Wir unterstützen diese Erweiterung. Die Zumutbarkeitsklausel beugt einem strukturellen Wettbewerbsnachteil kleiner Anbieter gegenüber großen Plattformen vor. Positiv ist zudem, dass der Normtext eine ausdrückliche Zweckbindung enthält – die Daten dürfen ausschließlich zur Erfüllung der BSI-Aufgaben nach § 3 Abs. 1 Nr. 1 und 2 verwendet werden – sowie eine Löschpflicht spätestens nach 24 Monaten.
Zwei Punkte bedürfen der Nachbesserung. Erstens: Soweit die übermittelten sicherheitsrelevanten Informationen im Einzelfall personenbezogene Daten enthalten – etwa IP-Adressen oder nutzerbezogene Metadaten –, fehlt eine explizite datenschutzrechtliche Verarbeitungsgrundlage im Normtext. Ob das der Fall ist, hängt vom Inhalt der jeweils abgefragten Information ab; eine pauschale Annahme von Personenbezug wäre falsch. Für die Fälle, in denen er vorliegt, muss die Rechtsgrundlage aber im Gesetz stehen, nicht im Ermessen der Behörde.
Zweitens fehlen – anders als bei § 8 BSIG für die Kommunikationstechnik des Bundes –

jegliche Anforderungen an die Sicherheit der Übertragungswege. § 15 Abs. 6 schweigt vollständig dazu, nach welchen technischen Standards die Informationen zu übermitteln sind. Die Gesetzesbegründung adressiert das für § 15 Abs. 6 ebenfalls nicht. Sicherheitsrelevante technische Informationen über Schwachstellen und Bedrohungslagen sind ihrem Wesen nach hochsensibel; ihre unsichere Übertragung schafft genau die Angriffsfläche, zu deren Behebung diese übertragen werden sollen. Wir fordern daher eine gesetzliche Verpflichtung zur Übertragung nach dem Stand der Technik sowie Beteiligung von IT-SicherheitsexpertInnen, der einschlägigen Hersteller und Betreiber bei der Festlegung der technischen (Schnittstellen-)Anforderungen.

# 3.2 abzulehnende Maßnahmen

Den Kern unserer Kritik bilden die in Artikel 2 (BPolG) und Artikel 4 (BKAG) vorgesehenen aktiven Cyberabwehrbefugnisse. Wir lehnen diese Regelungen ab. Nachfolgend begründen wir dies im Detail.

## 3.2.1 Verfügbarkeitsindikatoren und Angriffserkennung – § 31 Abs. 2 BSIG-neu

Der Entwurf fasst § 31 Abs. 2 BSIG neu und verpflichtet Betreiber kritischer Anlagen zur automatisierten Ausleitung von Betriebsdaten an das BSI. Das BMI bezeichnet diese Funktion im Begleitschreiben zur Verbändebeteiligung informell als „Heartbeat".

Der Mehrwert der Maßnahme ist marginal. Ihm steht eine konkrete, strukturell bedingte Vergrößerung der Angriffsfläche kritischer Anlagen gegenüber. Eine Auseinandersetzung mit dieser Abwägung enthält der Entwurf nicht.

Das BSI wird über bestehende Meldepflichten bereits im Eintrittsfall eines Vorfalls informiert und kann dann vorhandene Ressourcen einsetzen. Ein permanentes Echtzeit-Lagebild liefert gegenüber diesem etablierten Mechanismus keinen qualitativen Informationsgewinn – allenfalls einen kleinen zeitlichen Vorsprung.

Diesem fraglichen Mehrwert steht ein konkretes strukturelles Risiko gegenüber: Die Heartbeat-Verpflichtung zwingt Betreiber kritischer Anlagen, eine permanente Verbindung nach außen zu öffnen. KRITIS-Systeme sind nach dem Stand der Technik so konzipiert, dass ausgehende Verbindungen auf das betrieblich notwendige Minimum beschränkt werden. Jede zusätzliche Außenverbindung vergrößert die Angriffsfläche. Zusätzliche Risiken entstehen durch mögliche Fehlkonfiguration oder durch veraltete oder ungepatchte Systeme beim Betreibenden oder auf der Übertragungsstrecke. Diese Risiken sind keine theoretischen Szenarien, sondern dokumentierte Angriffsvektoren gegen kritische Infrastrukturen.

Wir fordern: Der Gesetzgeber soll darlegen, welchen konkreten operativen Mehrwert das Echtzeit-Lagebild gegenüber der bestehenden Meldepflicht bringt, und dabei nachweisen, dass dieser Mehrwert das durch die erzwungene zusätzliche Datenverbindung entstehende

Sicherheitsrisiko überwiegt. Solange dieser Nachweis nicht erbracht ist, lehnen wir § 31 Abs. 2 BSIG-neu ab.

### 3.2.2 Aktive Eingriffsbefugnisse von BKA und BPOL

Der Entwurf sieht für BKA (§ 62e BKAG-neu) und Bundespolizei (§ 41a BPolG-neu) die Befugnis vor, in informationstechnischen Systemen technische Daten zu erheben, zu verändern oder zu löschen. Diese Maßnahme zielt ausweislich der Entwurfsbegründung sowohl auf IT-Systeme von Angreifern als auch auf solche von Geschädigten (Opfersysteme). Darüber hinaus sieht der Entwurf die Befugnis zur Umleitung oder Unterbindung von Datenverkehr sowie zur Untersagung des Betriebs informationstechnischer Systeme vor. Das BKA erhält diese Befugnisse für alle bestehenden und neu geschaffenen Aufgaben, die Bundespolizei für alle ihre bestehenden Aufgaben.

Damit werden erstmals in der Geschichte der Bundesrepublik Polizeibehörden ermächtigt, ohne Wissen der Betroffenen aktiv in fremde IT-Systeme einzugreifen und dort Daten zu verändern oder zu löschen. Die Tragweite dieser Neuregelung wird im Entwurf systematisch unterschätzt.

### 3.2.3 Eingriff in Opfersysteme: Risiko für KRITIS

Die Entwurfsbegründung benennt ausdrücklich, dass aktive Eingriffe sowohl gegen Störersysteme als auch gegen Geschädigtensysteme (Opfersysteme) möglich sein sollen. Dies wurde in der Vergangenheit als offensichtlich verfassungswidrig identifiziert und als „Hackback“ bezeichnet und diskutiert und soll hier offenbar eingeführt werden.

Opfersysteme sind dabei IT-Systeme, die selbst kompromittiert wurden und von denen Schadsoftware weiter ausgeht – also etwa ein infizierter Server, der als Bot oder Proxy im Rahmen eines Botnetzes oder zur Verschleierung der Angriffsherkunft eingesetzt wird. Das ist ein operativ häufiges Szenario. Die Möglichkeit, dass KRITIS-Betreiber und sogar Behörden als ahnungslose Proxy-Infrastruktur für ausländische Angreifer instrumentalisiert werden, ist hier nicht mitgedacht worden.

Das bedeutet konkret: BKA oder BPOL wären berechtigt, in das IT-System eines deutschen KRITIS-Betreibers einzugreifen, dessen Systeme unter Verdacht stehen, kompromittiert worden zu sein. Dies würde ohne Wissen des Betreibers geschehen. Die Behörden hätten dabei sogar die Befugnis, Daten zu verändern oder zu löschen. Ein nicht abgestimmter Eingriff in Konfigurationsdaten, Systemparameter oder Netzwerkverbindungen kann dort unmittelbare Betriebsstörungen auslösen und bis zum Versorgungsausfall für die Bevölkerung führen. Der Entwurf adressiert dieses Risiko nicht.

### 3.2.4 Das Attributionsproblem: Angreiferinfrastruktur ist nahezu nie eindeutig identifizierbar

Der Entwurf behandelt die Attribution, also die Frage, welchem Akteur ein IT-System tatsächlich zuzurechnen ist, als ein im Wesentlichen gelöstes Problem. Die Gesetzesbegründung

behauptet, die Identifizierung des Angreifers sei „regelmäßig eindeutig möglich", weil IP-Adressen, Netzwerkmerkmale und Schadsoftwaresignaturen eine zuverlässige Zurechnung erlaubten. Diese Behauptung ist unhaltbar und fachlich falsch.

IP-Adressen und Netzwerkmerkmale identifizieren das Zwischensystem, von dem ein Angriff ausgeht, nicht den Angreifer dahinter. Die Angreiferinfrastruktur von organisierten kriminellen und anderen staatlichen und staatlich gesteuerten Akteuren besteht regelmäßig aus kompromittierten Systemen Dritter, deren Eigentümer selbst Opfer sind.

Viele Fälle belegen diesen Mechanismus, drei aussagekräftige Beispiele zum Beleg:

**SolarWinds/APT29 (Russland, 2020)**: Der russische Auslandsgeheimdienst SVR (APT29/Cozy Bear) kompromittierte die Build-Infrastruktur des Softwareanbieters SolarWinds und verteilte trojanisierte Updates an tausende Organisationen weltweit. Zu den infizierten Systemen zählten laut CISA sowohl US-Bundesbehörden als auch Betreiber amerikanischer kritischer Infrastrukturen, darunter nach NERC-Angaben[1] rund 25 % der amerikanischen Stromversorger. In Einzelfällen wurden Infektionen auch in OT- und ICS-Netzen detektiert. Die Angreifer operierten dabei über die Netzwerke der kompromittierten Opfer selbst — nicht über eigene, zurechenbare Infrastruktur. Die Zurechnung an den SVR erfolgte erst Monate nach Entdeckung, durch aufwendige forensische Analyse mehrerer Geheimdienste und Privatunternehmen gemeinsam, und wurde im April 2021 offiziell durch die US-Regierung erklärt. [2] [3]

**NotPetya/Sandworm (Russland, 2017)**: Die russische Gruppe Sandworm (TeleBots) kompromittierte vorab die Update-Server des ukrainischen Buchhaltungssoftware-Anbieters M.E.Doc, ein unbeteiligtes Drittunternehmen, und missbrauchte dessen legitimen Update-Mechanismus als Angriffsvektor. M.E.Doc war Opfer, nicht Täter. Der Angriff traf über 2.000 ukrainische Unternehmen sowie multinationale Konzerne weltweit. Wer im Moment des Angriffs die Netzwerkspur zurückverfolgte, landete bei den Servern eines ukrainischen Softwarehauses. [4] [5]

**Volt Typhoon/KV-Botnet (VR China, ab 2021)**: Die chinesische staatliche Gruppe baute ihre gesamte Befehls- und Steuerungsinfrastruktur aus kompromittierten SOHO-Routern privater Unternehmen und Haushalte auf — darunter Geräte der Hersteller Cisco, Netgear, ASUS und Fortinet. Der C2-Verkehr wurde durch Ketten solcher Fremdgeräte geleitet,

[1] NERC/Utility Dive, April 2021: https://www.utilitydive.com/news/nerc-finding-25-of-utilities-exposed-to-solarwinds-hack-indicates-growing/598449/
[2] Quellen: CISA Advisory AA20-352A, Dez. 2020: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
[3] CISA Statement on SolarWinds Attribution, 15. April 2021: https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise-closed
[4] Quellen: Cisco Talos, „The MeDoc Connection", Juli 2017: https://blog.talosintelligence.com/the-medoc-connection/
[5] Microsoft Security Blog, 27. Juni 2017: https://www.microsoft.com/en-us/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

bevor er die eigentliche Angreiferinfrastruktur erreichte. Wer einer Quell-IP-Adresse folgte, landete beim ahnungslosen Eigentümer eines abgekündigten Routers — nicht beim Angreifer. Das FBI musste im Januar 2024 per Gerichtsbeschluss in Hunderte kompromittierter US-amerikanischer Privatgeräte eingreifen, um das KV-Botnet zu zerschlagen. Diese Geräte und ihre Eigentümer waren selbst Opfer. Ein reaktiver staatlicher Gegenschlag auf die sichtbaren Quell-IP-Adressen hätte genau diese Opfer ein zweites Mal getroffen. [6] [7] [8]

Die drei Fälle belegen übereinstimmend: Angreiferinfrastruktur staatlicher Akteure kann strukturell aus kompromittierten Systemen Dritter bestehen. Die in §§ 62e BKAG-neu und 41a BPolG-neu vorgesehenen Eingriffsbefugnisse sind auf dieser Grundlage strukturell falsch kalibriert: Sie ermächtigen dazu, Opfer zu treffen.

Staatliche Eingriffsbefugnisse, die auf solch unsicherer Attributionsgrundlage ausgeübt werden, treffen mit hoher Wahrscheinlichkeit die falschen Systeme und können unvorhersehbare Folgen auslösen.

Die Konsequenz wäre: Der Staat greift in die IT-Infrastruktur von KRITIS-Betreibern oder anderen deutschen Unternehmen ein, die Opfer eines Angriffs sind – und verursacht selbst einen Schaden, dessen Folgen bei kritischer Infrastruktur nicht absehbar sind und immer wieder zu Versorgungsausfällen der Bevölkerung führen werden.

## 3.2.5 § 3a BKAG-neu: Kompetenzverschiebung ohne verfassungsrechtliche Grundlage

Die neue Aufgabennorm des § 3a BKAG-neu ist verfassungsrechtlich in mehrfacher Hinsicht fragwürdig. Der Begriff der außen- und sicherheitspolitischen Bedeutung eines Cyberangriffs ist ein unbestimmter Rechtsbegriff, der dem BKA einen im Wesentlichen unkontrollierbaren Beurteilungsspielraum einräumt. Da praktisch jeder staatliche Cyberangriff mit relevanter Zielrichtung außen- und sicherheitspolitische Implikationen aufweist, droht § 3a BKAG-neu zu einer allgemeinen Bundeszuständigkeit für Cyberabwehr zu werden.

Damit verletzt der Entwurf das bundesstaatliche Kompetenzgefüge des Grundgesetzes. Die Gefahrenabwehr ist nach Art. 30 GG grundsätzlich Ländersache. Eine Bundeskompetenz bedarf einer ausdrücklichen Grundlage im Grundgesetz. Für das BKA ist diese in Art. 73 Abs. 1 Nr. 9a

[6] CISA/NSA/FBI Joint Advisory AA23-144A, 24. Mai 2023: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
[7] CISA/NSA/FBI Joint Advisory AA24-038A, 7. Februar 2024: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
[8] U.S. Department of Justice, „Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China", 31. Januar 2024: https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

GG (Abwehr des internationalen Terrorismus) und Nr. 10 GG (internationale Verbrechensbekämpfung) verankert. Die Erstreckung auf Cyberangriffe von außen- und sicherheitspolitischer Bedeutung übersteigt den Rahmen dieser Normen: Sie schafft eine allgemeine Bundeszuständigkeit für Cyberangriffe auf der Grundlage eines politischen Bedeutungskriteriums, das im Grundgesetz keine Entsprechung hat. Die Gesetzgebungskompetenz des Bundes aus der „Natur der Sache“, auf die der Entwurf in der Begründung abstellt, ist nach der Rechtsprechung des Bundesverfassungsgerichts eng auszulegen und auf Aufgaben beschränkt, die ihrer Natur nach nur bundeseinheitlich erfüllt werden können. Das trifft auf die allgemeine Abwehr von Cyberangriffen mit „außen- und sicherheitspolitischer Bedeutung" nicht zu. Diese Begründung trägt verfassungsrechtlich nicht.

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts ist die Kompetenz kraft „Natur der Sache" auf Sachgebiete beschränkt, die strukturell nur bundeseinheitlich geregelt werden können und bei denen eine Länderzuständigkeit von vornherein ausscheidet (BVerfGE 12, 205). Anerkannte Anwendungsfälle sind Bundeshauptstadt, Nationalflagge und ähnliche Materien, die das Bundesstaatswesen als solches konstituieren. Praktische Zweckmäßigkeit einer bundeseinheitlichen Regelung, oder die Tatsache, dass ein Angriff transnationale Bezüge aufweist, genügt nicht.

Polizeiliche Gefahrenabwehr ist nach Art. 30, 70 GG Ländersache. Der transnationale Charakter eines Cyberangriffs und seine außenpolitischen Implikationen machen ihn nicht zu einer Materie, die strukturell unausweichlich bundeseinheitlich geregelt werden müsste. Für BKA-Kompetenzen in transnationalen Bedrohungslagen hat das Grundgesetz ausdrückliche Kompetenztitel geschaffen — namentlich Art. 73 Abs. 1 Nr. 9a GG (internationaler Terrorismus) und Art. 73 Abs. 1 Nr. 10 GG (kriminalpolizeiliche Zusammenarbeit). Soweit diese Titel für neue Bedrohungslagen nicht ausreichen, ist der Weg einer Verfassungsänderung nach Art. 79 GG geboten — nicht der Rückgriff auf eine ungeschriebene Kompetenz, die das BVerfG auf absolute Ausnahmefälle beschränkt.

Darüber hinaus fehlt eine klare Abgrenzung zu den bestehenden Zuständigkeiten des Verfassungsschutzes, des Bundesnachrichtendienstes und der Bundeswehr im Cyberraum. Der Entwurf schafft institutionelle Überschneidungen, ohne Koordinationsmechanismen verbindlich zu regeln, und lädt damit zu Kompetenzstreitigkeiten und operativen Konflikten ein. Das bereits vorhandene Cyber-Wimmelbild der Verantwortungsdiffusion wird dadurch weiter verstärkt.

## 3.2.6 Fehlende Evaluations- und Befristungsklausel

Der Entwurf sieht ausdrücklich weder eine Befristung noch eine gesetzlich verankerte Evaluation der neuen Eingriffsbefugnisse vor. Die Begründung lautet, die Regelungen knüpften an bestehende Rechtsstrukturen an und ihre Auswirkungen seien „im Wesentlichen prognostizierbar“. Das ist für Befugnisse dieser Art unzureichend. Aktive Eingriffe in fremde IT-Systeme durch Polizeibehörden haben in Deutschland keine historischen Anwendungsbeispiele. Ihre tatsächlichen Auswirkungen auf die Sicherheitslage kritischer

Infrastrukturen sind ex ante nicht vollständig beurteilbar. Eine Evaluationsklausel mit klarer Berichtspflicht gegenüber dem Deutschen Bundestag nach drei Jahren ist nicht optional. Diese wäre eine Mindestanforderung für verantwortungsvolle Gesetzgebung in einem neuen, nicht erprobten aber offensiven Eingriffsbereich.

## 3.3 Strukturelle Warnung: Der Weg in offensive Cyberoperationen

Die AG KRITIS weist ausdrücklich darauf hin, dass die im Entwurf vorgesehenen aktiven Eingriffsbefugnisse strukturell denselben Pfad einschlagen wie der politisch diskutierte „Hackback“. Der Entwurf vermeidet den Begriff – die Sache ist jedoch dieselbe.

Eine wirksame aktive Cyberabwehr - also offensive Angriffe gegen fremde IT-Systeme - gegen Infrastrukturen von angreifenden Akteuren setzt voraus, dass Mittel entwickelt und eingesetzt werden, mit denen sich gezielt Schwachstellen ausnutzen lassen.

Solche Schwachstellen betreffen jedoch häufig Standard-Systeme, -software und -komponenten, die nicht nur von Angreifenden, sondern zugleich von einer unbekannten Zahl potenzieller Opfer, als auch von der deutschen Wirtschaft selbst genutzt werden. Werden diese Sicherheitslücken durch offensiv tätige Behörden ausgenutzt, statt diese umgehend durch den Hersteller schließen zu lassen, entsteht ein erhebliches Gefahrenpotenzial.

Besonders kritisch ist die Lage in sensiblen Bereichen: Kritische Infrastrukturen arbeiten vielfach mit Standard-Systemen, -software und -komponenten, aber auch mit OT- und ICS-Systemen, die weltweit nur von wenigen Herstellern produziert werden. Entscheidet sich der Staat, Kenntnisse über Schwachstellen für offensive Zwecke zurückzuhalten, bleiben kritische Infrastrukturen, wie zum Beispiel (Wasser-)Kraftwerke, Flughäfen oder Krankenhäuser ungeschützt.

Die Risiken eines solchen staatlichen Handelns sind nicht theoretisch: Staatlich entwickelte und eingesetzte Schadsoftware kann sich unkontrolliert verbreiten. Ein Beispiel ist die von Geheimdiensten aus USA und Israel entwickelte Schadsoftware Stuxnet (2010), die sich über ihr ursprüngliches Ziel (iranische Urananreicherungsanlagen) hinaus in industrielle Steuerungsanlagen weltweit verbreitete, darunter auch sehr viele Systeme in nicht am Konflikt beteiligten Staaten.

Solche Schadsoftware kann zudem forensisch analysiert, weiterentwickelt und gegen deutsche Infrastruktur eingesetzt werden.

Wer staatliche Schadsoftware zum Ausnutzen von Sicherheitslücken entwickelt, um Systeme abzuschalten, darf nicht überrascht sein, wenn diese Schadsoftware später gegen deutsche kritische Infrastruktur eingesetzt wird. Das Angriffsmittel wird als Bedrohung zurückkehren.

Hinzu kommt ein strukturelles Risiko: Die Einführung aktiver Eingriffsbefugnisse führt zwangsläufig zum Aufbau entsprechender Fähigkeiten bei Sicherheitsbehörden wie dem

Bundeskriminalamt und der Bundespolizei. Dazu gehören detaillierte Kenntnisse über Schwachstellen, die Entwicklung von ausnutzender Schadsoftware (Exploits) sowie der Einsatz von Software zum Eindringen in fremde Systeme.

Nicht der einzelne Einsatz, sondern dieser dauerhafte Kapazitätsaufbau stellt eine zusätzliche Gefährdung dar. Solche Fähigkeiten sind faktisch irreversibel. Einmal etabliert, unterliegen sie institutionellen Eigeninteressen und werden erfahrungsgemäß schrittweise ausgeweitet.

Der Entwurf muss darlegen, durch welchen konkreten Mechanismus verhindert wird, dass der Aufbau aktiver Eingriffsfähigkeiten bei BKA und BPOL zum Aufbau eines staatlichen Schwachstellenpools führt. Darüber hinaus ist die Haftungsfrage ungeklärt, ob und wie BKA oder BPOL eine Haftung übernehmen, wenn durch deren Zurückhalten von Schwachstellen eine kritische Infrastruktur in Deutschland und aufgrund dessen dann auch Teile der Bevölkerung zu Schaden kommen. Solche Darlegungen fehlen vollständig. Solange sie fehlen, ist der Entwurf in den Teilen, die aktive Eingriffe betreffen, mit dem Ziel der Versorgungssicherheit der Bevölkerung, der IT-Sicherheit und dem Schutz von KRITIS unvereinbar.

## 3.4 Strukturelle Defizite des Entwurfs

### 3.4.1 Unzureichender Richtervorbehalt

Der Entwurf sieht einen Richtervorbehalt für Maßnahmen nach § 62e BKAG-neu (verdeckter Eingriff in IT-Systeme) nur für den Eingriff in private informationstechnische Systeme vor. Für den Eingriff in nicht-private Systeme — also in Systeme von Behörden, der deutschen Wirtschaft und insbesondere KRITIS-Betreibern — fehlt ein Richtervorbehalt vollständig.

Diese Differenzierung ist verfassungsrechtlich nicht begründbar. Der Vergleich mit bestehenden Regelungen zeigt, dass der Gesetzgeber für strukturell weniger einschneidende verdeckte Eingriffe in IT-Systeme durchgängig einen Richtervorbehalt für erforderlich hält, ohne Ausnahme für den institutionellen oder betrieblichen Kontext:

Für die Strafverfolgung regeln § 100a StPO (Quellen-TKÜ) und § 100b StPO (Online-Durchsuchung) verdeckte Eingriffe in IT-Systeme unter obligatorischem Richtervorbehalt nach § 100e StPO. Das gilt unabhängig davon, ob das betroffene Gerät privat oder betrieblich genutzt wird.

Für die präventive Terrorismusabwehr durch das BKA gilt dasselbe: § 49 BKAG (Online-Durchsuchung) und § 51 BKAG (Quellen-TKÜ) setzen jeweils eine richterliche Anordnung voraus, ohne Ausnahme für Unternehmensnetze oder Infrastrukturbetreiber.

Der neue § 62e BKAG-neu ermächtigt demgegenüber zu Dateneingriffen, die in ihrer Intensität die Online-Durchsuchung übertreffen, da sogar Veränderung und Löschung von Daten, der verdeckte Zugriff ohne Wissen des Betreibers und Eingriffe in OT-Systeme (in der Prozessautomatisierung von Produktionsanlagen und Fabriken) ermöglicht werden.

Ein sachlicher Grund dafür, warum das Leitsystem eines Stromnetzbetreibers oder eines Wasserwerks weniger Richtervorbehaltsschutz genießen soll als der private Laptop eines Einzelnen, ist nicht erkennbar und wird im Entwurf auch nicht dargelegt.

### 3.4.2 Haftung für Kollateralschäden

Der Entwurf enthält keine Regelung zur Haftung des Staates für verursachte Material- und Personen-Schäden, die durch fehlerhafte oder fehlgeleitete aktive Cyberabwehrmaßnahmen entstehen. Dies betrifft nicht nur unmittelbare Schäden an dem einbezogenen IT-System selbst, sondern vor allem mittelbare Schäden an Dritten. Wenn eine staatliche Cyberabwehrmaßnahme dazu führt, dass ein KRITIS-Betreiber seine Versorgungsleistung an die Bevölkerung auch nur temporär unterbricht, können Schäden bei einer Vielzahl von - insbesondere vulnerablen - Bevölkerungsgruppen, Unternehmen, Einrichtungen und Behörden entstehen.

Haushalte ohne Strom, Unternehmen ohne Betriebswasser, Krankenhäuser ohne verlässliche Steuerungssysteme, Berlin ohne Strom: Das sind die realen Risiken und Gefahren eines durch staatliche Eingriffe ausgelösten Versorgungsausfalls der Bevölkerung. Die Frage ist dabei nicht, ob, sondern wann und wie oft diese eintreten werden.

Weder der unmittelbar betroffene Betreiber, noch mittelbar geschädigte Unternehmen und Bürgerinnen und Bürger verfügen nach aktuellem Recht über eine eindeutige Rechtsgrundlage für Schadensersatzansprüche gegen den Staat. Die allgemeine Linie aus dem BGH-Fallrecht ist keine ausreichende Grundlage für die komplexen Schadenslagen, die ein durch Cyberabwehr ausgelöster Versorgungsausfall für die Bevölkerung erzeugen kann.

Unsere Forderung lautet daher: Schaffung einer spezialgesetzlichen Haftungsgrundlage für unmittelbare und mittelbare Schäden, die durch Maßnahmen nach §§ 62c–62g BKAG-neu und § 41a BPolG-neu verursacht werden – einschließlich Schadensersatzansprüchen Dritter (Bevölkerung, Unternehmen, KRITIS), die einen Schaden, verursacht durch einen Versorgungsausfall, erleiden.

# 4 Fazit und Zusammenfassung

Der vorliegende Referentenentwurf enthält sowohl Maßnahmen, die die AG KRITIS ausdrücklich unterstützt, als auch solche, die sie aus strukturellen Gründen entschieden ablehnt.

Was der Entwurf richtig macht: Die Fortentwicklung der Schadprogrammerkennung nach § 8 BSIG, die Erweiterung der BSI-Unterstützungsbefugnis auf Früherkennungsfälle nach § 11 Abs. 1 BSIG-neu sowie die Anordnungsbefugnisse gegenüber DNS-Anbietern sind defensiv, im Grundsatz verhältnismäßig und bei sachgerechter Ausgestaltung betrieblich integrierbar. Wir unterstützen diese Maßnahmen, verbinden diese aber im Einzelnen explizit mit den erforderlichen Nachbesserungen.

Was der Entwurf grundlegend falsch macht: Die aktiven Eingriffsbefugnisse für BKA und Bundespolizei nach §§ 62c–62g BKAG-neu und § 41a BPolG-neu sind mit dem Ziel der Versorgungssicherheit der Bevölkerung und der Sicherheit kritischer Infrastrukturen strukturell unvereinbar. Die AG KRITIS lehnt diese Befugnisse daher explizit ab. Die Gründe sind nicht rechtspolitischer Natur, sie sind operativ-technisch und verfassungsrechtlich:

**Erstens**: Der Entwurf ermächtigt Bundeskriminalamt und Bundespolizei ausdrücklich zu Eingriffen in Opfersysteme. Also IT-Systeme, die selbst Ziel eines Angriffs waren und dadurch als Angriffsinfrastruktur missbraucht werden. Da KRITIS-Betreiber und deren Zulieferer in der dokumentierten Praxis staatlicher Angreifer regelmäßig als ahnungslose Proxy-Infrastruktur instrumentalisiert werden (SolarWinds/APT29, NotPetya/Sandworm, Volt Typhoon/KV-Botnet), würden diese Befugnisse mit hoher Wahrscheinlichkeit genau die Systeme treffen, die der Staat zu schützen vorgibt. Der Entwurf enthält keinen Mechanismus, der dies verhindert.

**Zweitens**: Die Behauptung der Gesetzesbegründung, Attribution sei „regelmäßig eindeutig möglich", ist fachlich falsch. Angreiferinfrastruktur von organisierten kriminellen und anderen staatlichen Akteuren besteht strukturell aus kompromittierten Systemen Dritter. Die sichtbare Quell-IP-Adresse identifiziert nicht die angreifenden Akteure, sondern deren Opfer. Ein Eingriff auf dieser Grundlage ist ein Eingriff gegen das falsche Ziel.

**Drittens**: Der Aufbau aktiver Eingriffsfähigkeiten bei BKA und BPOL erzwingt den Aufbau eines staatlichen Schwachstellenpools. Jede Schwachstelle, die für offensive Maßnahmen zurückgehalten wird, hält auch die deutsche Wirtschaft und kritische Infrastrukturen ungeschützt und angreifbar. Schadsoftware, die staatlich entwickelt wird, kann unkontrolliert streuen und gegen deutsche Wirtschaft und kritische Infrastrukturen eingesetzt werden. Stuxnet (2010) belegt dies. Ein weiteres Beispiel ist die Schadsoftware notpetya, die sich durch eine von der US-Regierung zurückgehaltene Sicherheitslücke (EternalBlue) verbreiten konnte. Dieser Kapazitätsaufbau ist irreversibel und unterliegt dem institutionellen Eigeninteresse seiner Träger.

**Viertens**: Der Entwurf sieht für Eingriffe in nicht-private IT-Systeme — also in Systeme von Unternehmen, Stromnetzbetreibern, Flughäfen, Krankenhäusern, (Wasser-)Kraftwerken und sonstigen KRITIS-Betreibern — keinen Richtervorbehalt vor. Das ist verfassungsrechtlich nicht begründbar. Das Leitsystem eines Stromnetzbetreibers verdient nicht weniger Schutz als der private Laptop eines Einzelnen — es benötigt mehr Schutz.

**Fünftens**: Der Entwurf enthält weder eine Evaluations- und Befristungsklausel noch eine spezialgesetzliche Haftungsregelung für Kollateralschäden. Wenn eine staatliche Cyberabwehrmaßnahme einen Versorgungsausfall für die Bevölkerung auslöst, haben weder der betroffene Betreiber noch die geschädigte Bevölkerung nach geltendem Recht eine klare Grundlage für Schadensersatzansprüche gegen den Staat. Dieser Zustand ist rechtsstaatlich nicht akzeptabel.

**Sechstens**: Die neue Aufgabennorm des § 3a BKAG-neu schafft über den unbestimmten Rechtsbegriff der „außen- und sicherheitspolitischen Bedeutung" faktisch eine allgemeine Bundeszuständigkeit für Cyberangriffe, ohne dass hierfür eine ausreichende verfassungsrechtliche Grundlage im Grundgesetz besteht. Die Kompetenz der Länder zur Gefahrenabwehr nach Art. 30 GG wird damit systematisch ausgehöhlt.

**Diese Befugnisse sind nicht nachbesserungsfähig**.

Es gibt keine Ausgestaltung, keine Verfahrensgarantie, keinen Richtervorbehalt und keine Kontrollstruktur, die das strukturelle Problem löst: **Wer offensive Cyberkapazitäten aufbaut, gefährdet die eigene Infrastruktur.**

Wer Schwachstellen zurückhält, lässt deutsche KRITIS ungeschützt. Wer in Opfersysteme eingreift, trifft die Falschen. Das ist keine Frage der Ausgestaltung, das ist die Logik offensiver Cyberoperationen selbst.

Der Entwurf ist in den Teilen, die aktive Eingriffsbefugnisse betreffen, nicht reformierbar — er ist in diesen Teilen falsch. Wer Strafverfolgungsbehörden ermächtigt in fremde IT-Systeme einzugreifen, Daten zu verändern oder zu löschen und Systeme abzuschalten, schafft keinen Schutz für die Bevölkerung. Er schafft eine staatliche Bedrohung für die Wirtschaft und kritischen Infrastrukturen, von der diese Bevölkerung abhängt.

Die AG KRITIS fordert das Bundesministerium des Innern mit Nachdruck auf: **Streichen Sie §§ 62c–62g BKAG-neu und § 41a BPolG-neu ersatzlos. Nicht überarbeiten. Streichen.**