GESELLSCHAFT
FÜR INFORMATIK

Berlin, 16. März 2026

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zum Referentenentwurf des Bundesministeriums des Innern (BMI) für das Gesetz zur Stärkung der Cybersicherheit

GESELLSCHAFT
FÜR INFORMATIK

Die Gesellschaft für Informatik e.V. (GI) nimmt zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung der Cybersicherheit vom 24. Februar 2026 wie folgt Stellung.

Die GI begrüßt das Ziel des Gesetzgebers, die Cybersicherheit in Deutschland zu stärken und die Erkennungs- und Abwehrfähigkeiten gegen Cyberangriffe auszubauen. Angesichts der dynamischen Bedrohungslage ist ein gesetzgeberisches Handeln grundsätzlich geboten. Der vorliegende Entwurf enthält sowohl sachgerechte, unterstützenswerte Maßnahmen im Bereich des BSI-Gesetzes als auch Regelungen, die die GI aus informatisch-technischer und grundrechtlicher Perspektive für hochproblematisch hält.

- Der Entwurf vollzieht einen Paradigmenwechsel: Cybersicherheit wird nicht mehr vorrangig als Frage von Schutz, Prävention und Resilienz verstanden, sondern zunehmend als Legitimation für staatliche Eingriffe in Netze und IT-Systeme. Die GI hält an ihrer Position fest, dass IT-Sicherheit präventiv gestaltet werden muss und intrusive Maßnahmen wie sogenannte Hackbacks abzulehnen sind. .

- Der Entwurf greift tief in die Architektur und Steuerungslogik digitaler Infrastrukturen ein. Wenn mit BKA, Bundespolizei und BSI künftig drei Bundesakteure weitreichende Eingriffsbefugnisse in informationstechnische Systeme erhalten, stellt sich die Frage nach wirksamen rechtsstaatlichen Kontrollmechanismen, klaren Zuständigkeitsabgrenzungen und nach den tatsächlichen Auswirkungen auf die IT-Sicherheit in Deutschland. Die GI differenziert in ihrer Bewertung daher ausdrücklich zwischen den defensiv angelegten BSI-Befugnissen, die wir grundsätzlich unterstützen, und den aktiven Eingriffsbefugnissen für BKA und Bundespolizei, die wir aus fachlichen und verfassungsrechtlichen Gründen ablehnen.

1. Die Schaffung von Rechtsgrundlagen für Cyberabwehrbefugnisse von BKA und BPOL

Der Entwurf schafft erstmals gesetzliche Grundlagen für aktive Cyberabwehrbefugnisse von Bundeskriminalamt und Bundespolizei. Beide Behörden sollen für ihre bestehenden Aufgaben Befugnisse zur Umleitung oder Unterbindung von Datenverkehr, zur Untersagung oder Einschränkung des Betriebs informationstechnischer Systeme sowie zum Auslesen, Löschen oder Verändern von Daten in IT-Systemen erhalten – auch durch verdeckten Eingriff mit technischen Mitteln und ohne Wissen der Betroffenen. Das BKA erhält diese Befugnisse zudem für die vorgesehene Aufgabe der Abwehr von Cybergefahren bei internationaler Zusammenarbeit oder außen- und sicherheitspolitischer Bedeutung.

Die GI lehnt die vorgesehenen aktiven Eingriffsbefugnisse für BKA und Bundespolizei ab. Die Gründe hierfür sind sowohl technischer als auch verfassungsrechtlicher Natur.

Struktureller Zielkonflikt durch offensive Fähigkeiten: Die GI hat bereits 2019 im Rahmen des IT-Sicherheitsgesetzes 2.0 und 2022 in ihrem Policy Brief zur aktiven Cyberabwehr darauf hingewiesen, dass eine Behörde sich nicht glaubhaft für das Schließen von Sicherheitslücken einsetzen kann, wenn sie gleichzeitig auf eben diese Schwachstellen angewiesen ist, um offensive Szenarien zu verfolgen. Dieser Zielkonflikt verschärft sich mit dem vorliegenden Entwurf erheblich: Der Aufbau aktiver Eingriffsfähigkeiten bei BKA und Bundespolizei erzwingt den Aufbau eines staatlichen Schwachstellen-Pools. Jede Sicherheitslücke, die für offensive Maßnahmen zurückgehalten wird, lässt die deutsche Wirtschaft und kritische Infrastrukturen ungeschützt. Die GI fordert stattdessen ein wirksames Schwachstellen Management, das auf die Schließung aller bekannten Sicherheitslücken ausgerichtet ist.

Ungelöstes Attributionsproblem: Die in der Gesetzesbegründung aufgestellte Behauptung, die Identifizierung von Angreifern sei „regelmäßig eindeutig möglich“, ist aus informatischer Sicht nicht haltbar. IP-Adressen und Netzwerkmerkmale identifizieren lediglich das Zwischensystem, von dem ein Angriff ausgeht, nicht den tatsächlichen Angreifer. Angreiferinfrastrukturen staatlicher und nicht-Staatlicher Akteure bestehen regelmäßig aus kompromittierten Systemen Dritter. Prominente Beispiele wie SolarWinds/APT29, NotPetya/Sandworm und Volt Typhoon belegen, dass Angreifer systematisch die Systeme unbeteiligter Dritter als Proxy-Infrastruktur missbrauchen. Ein staatlicher Eingriff auf Basis solch unsicherer Attribution trifft mit hoher Wahrscheinlichkeit die falschen Systeme.

Gefährdung kritischer Infrastrukturen durch Eingriffe in Opfersysteme: Der Entwurf ermächtigt BKA und Bundespolizei ausdrücklich zu Eingriffen sowohl in Störer- als auch in Opfersysteme. Da KRITIS-Betreiber in der dokumentierten Praxis staatlicher Angreifer regelmäßig als ahnungslose Proxy-Infrastruktur instrumentalisiert werden, würden diese Befugnisse mit hoher Wahrscheinlichkeit genau die Systeme treffen, die der Staat zu schützen vorgibt. Ein nicht abgestimmter Eingriff in Konfigurationsdaten,

Systemparameter oder Netzwerkverbindungen kann bei kritischen Infrastrukturen unmittelbare Betriebsstörungen bis hin zum Versorgungsausfall auslösen.

Normalisierung der Instrumente der Netzsteuerung: Die im Entwurf vorgesehenen DNS- und Routing-Eingriffe sowie staatlich angeordnete Traffic-Umleitungen auf polizeilich kontrollierte Systeme (Sinkholes) schaffen eine technische Infrastruktur, die strukturell geeignet ist, Kommunikationsflüsse zentral zu beeinflussen. Diese Mechanismen wurden bisher vorwiegend im Kontext von Zensur- und Kontrollregimen diskutiert. Ihre gesetzliche Normalisierung in Deutschland untergräbt die Glaubwürdigkeit in der internationalen Debatte über digitale Freiheitsrechte.

Unzureichender Richtervorbehalt: Der Entwurf sieht einen Richtervorbehalt nur für Eingriffe in private informationstechnische Systeme vor. Für den verdeckten Eingriff in nicht-private Systeme, also in Systeme von Unternehmen, KRITIS-Betreibern und Behörden, fehlt jeder Richtervorbehalt. Dies ist nicht nachvollziehbar, denn die vorgesehenen Eingriffe beeinträchtigen die Grundrechtspositionen der Betreiber. Zudem beeinträchtigen Eingriffe in die von ihnen betriebenen Systeme regelmäßig direkt oder indirekt auch die Grundrechte der jeweiligen (individuellen) Nutzenden. Angesichts der Vielzahl der Betroffenen kann die Eingriffstiefe derartiger Befugnisse sogar größer sein als bei der Infiltration eines privaten Systems: Das Leitsystem eines Stromnetzbetreibers oder eines Krankenhauses verdient mindestens denselben richterlichen Schutz wie der private Laptop eines Einzelnen. Für strukturell weniger einschneidende Eingriffe wie die Online-Durchsuchung (§ 100b StPO) oder die Quellen-TKÜ (§ 100a StPO) besteht ein obligatorischer Richtervorbehalt unabhängig vom Kontext.

Verfassungsrechtlich fragwürdige Kompetenzerweiterung nach § 3a BKAG-neu: Der unbestimmte Rechtsbegriff der „außen- und sicherheitspolitischen Bedeutung“ droht zu einer faktisch allgemeinen Bundeszuständigkeit für Cyberabwehr zu führen. Da nahezu jeder staatliche Cyberangriff mit relevanter Zielrichtung außen- und sicherheitspolitische Implikationen aufweist, wird das föderale Kompetenzgefüge des Grundgesetzes unterlaufen. Die Gefahrenabwehr ist nach Art. 30 GG grundsätzlich Ländersache. Zudem schafft der Entwurf institutionelle Überschneidungen mit den Zuständigkeiten von Verfassungsschutz, BND und Bundeswehr im Cyberraum, ohne Koordinationsmechanismen verbindlich zu regeln.

Fehlende Evaluationsklausel und Haftungsregelung: Aktive Eingriffe in fremde IT-Systeme durch Polizeibehörden haben in Deutschland keine historischen Anwendungsbeispiele. Ihre Auswirkungen sind ex ante nicht vollständig beurteilbar. Die Behauptung des Entwurfs, die Auswirkungen seien „im Wesentlichen prognostizierbar“, ist nicht überzeugend. Die GI fordert eine gesetzlich verankerte Evaluierungspflicht mit klarer Berichtspflicht gegenüber dem Deutschen Bundestag nach spätestens drei Jahren. Der Bundesrechnungshof hat im Zusammenhang mit der Cybersicherheitsstrategie bereits das Fehlen einer systematischen Erfolgskontrolle moniert. Zudem fehlt jede spezialgesetzliche Haftungsregelung für Schäden, die durch

fehlerhafte Cyberabwehrmaßnahmen entstehen – insbesondere für mittelbare Schäden an der Bevölkerung durch Versorgungsausfälle.

Empfehlung der GI: *Die GI empfiehlt, die aktiven Eingriffsbefugnisse nach §§ 62c–62g BKAG-neu und § 41a BPolG-neu ersatzlos zu streichen. Cyberabwehr sollte sich auf nicht-intrusive Maßnahmen beschränken. Intrusive Maßnahmen und das Geheimhalten von Schwachstellen gefährden die IT-Sicherheit der gesamten Gesellschaft. Stattdessen sollte der Gesetzgeber in Prävention, ein wirksames Schwachstellenmanagement, Verschlüsselung und die personelle und technische Stärkung des BSI investieren.*

2. Stärkung der Cybersicherheit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Der Entwurf sieht eine erhebliche Ausweitung der Befugnisse und Fähigkeiten des BSI vor. Die Maßnahmen umfassen Verbesserungen am Schadprogramm-Erkennungssystem zum Schutz der Kommunikationstechnik des Bundes, den Einsatz von Incident Response Teams des BSI bereits bei Verdacht auf vorbereitendes Eindringen von Angreifern (Prepositioning), neue Anordnungsbefugnisse gegenüber DNS-Diensteanbietern und Registraren sowie die Verpflichtung von TK- und digitalen Diensteanbietern, dem BSI sicherheitsrelevante technische Informationen bereitzustellen. Hinzu kommt die automatisierte Ausleitung von Verfügbarkeitsindikatoren und Daten zur Angriffserkennung aus kritischen Anlagen an das BSI.

Die GI begrüßt die Stärkung des BSI grundsätzlich. Im Einzelnen:

Schadprogrammerkennung (§ 8 BSIG): Die Verbesserungen am Schadprogramm-Erkennungssystem zum Schutz der Kommunikationstechnik des Bundes sind sachgerecht. Die Ausweitung der Speicherfrist ist operativ nachvollziehbar, da Angriffskampagnen regelmäßig über Monate unentdeckt laufen. Die Maßnahme operiert ohne aktive Eingriffsbefugnisse in fremde Systeme und ist rein auf Detektion ausgerichtet. Die GI unterstützt diese Anpassung.

Früherkennungsfälle und Prepositioning (§ 11 BSIG): Die Erweiterung der BSI-Unterstützungsbefugnis auf Fälle, in denen Angreifer bereits in Systeme eingedrungen sind, aber noch keinen sichtbaren Schaden verursacht haben (Prepositioning), ist operativ geboten und wird von der GI unterstützt. Die bisherige Beschränkung auf eingetretene Beeinträchtigungen ist nicht mehr zeitgemäß. Entscheidend ist, dass die Regelung das Ersuchen der betroffenen Einrichtung als Voraussetzung beibehält.

DNS-Anordnungsbefugnisse (§§ 16a, 17 Abs. 2 BSIG-neu): Die Befugnisse gegenüber DNS-Anbietern und Registraren sind grundsätzlich sachgerecht und entsprechen internationalem Standard. Positiv ist die Unterrichtungspflicht gegenüber dem bzw. der Bundesdatenschutzbeauftragten. Die GI regt an, den Verpflichtetenkreis in § 17 Abs. 2 verständlicher zu beschreiben und eine Dokumentationspflicht über Umfang und Begründung einzelner Anordnungen gegenüber dem Deutschen Bundestag einzuführen.

Informationspflichten für TK- und digitale Diensteanbieter (§ 15 Abs. 6 BSIG-neu): Die Erweiterung der Auskunftspflichten ist sachgerecht und wird von der GI unterstützt. Die Zumutbarkeitsklausel und die Zweckbindung sind positiv zu bewerten. Die GI weist darauf hin, dass im Normtext gesetzliche Anforderungen an die Sicherheit der Übertragungswege fehlen. Sicherheitsrelevante technische Informationen über Schwachstellen und Bedrohungslagen sind hochsensibel; ihre unsichere Übertragung schafft genau die Angriffsfläche, zu deren Behebung sie erhoben werden. Es wird angeregt, den Entwurf um die Verpflichtung zum Treffen von entsprechenden Sicherheitsmaßnahmen nach dem Stand der Technik zu verpflichten.

Heartbeat-Pflicht und Angriffserkennung bei KRITIS (§ 31 Abs. 2 BSIG-neu): Die Verpflichtung zur automatisierten Ausleitung von Verfügbarkeitsindikatoren und Betriebsdaten an das BSI betrachtet die GI kritisch. KRITIS-Systeme sind nach dem Stand der Technik so konzipiert, dass ausgehende Verbindungen auf das betrieblich notwendige Minimum beschränkt werden. Jede zusätzliche permanente Außenverbindung vergrößert die Angriffsfläche. Dem fraglichen Mehrwert gegenüber den bestehenden Meldepflichten steht ein konkretes strukturelles Sicherheitsrisiko gegenüber. Die GI empfiehlt dem Gesetzgeber, den konkreten operativen Mehrwert gegenüber bestehenden Meldepflichten zu überprüfen. Eine doppelte Definition von Systemen zur Angriffserkennung im BSIG-E ist zudem entbehrlich, da diese in der Orientierungshilfe des BSI (OH SzA) bereits ausführlich definiert werden. Die Handhabung der Vielzahl unterschiedlicher Meldepflichten (NIS-2, KRITIS-DachG, DSGVO) wird durch die vorgesehene automatisierte Ausleitung nicht vereinfacht, sondern faktisch weiter kompliziert. Die GI hat bereits in früheren Stellungnahmen eine Vereinheitlichung und Reduktion der Komplexität bei Meldepflichten empfohlen.

Empfehlung der GI: *Die GI unterstützt es, das BSI mit ausreichend Personal und Ressourcen ausstatten, um Informationen aus den Meldesystemen auszuwerten und mit Handlungsempfehlungen oder Unterstützung reagieren zu können. Die Hürden im Meldesystem des BSI sollten abgebaut werden. Viele Daten allein ergeben noch kein Lagebild – entscheidend ist die Fähigkeit zur qualifizierten Auswertung und zur Ableitung konkreter Maßnahmen. Die Stärkung des BSI muss mit einer unabhängigen Evaluation der bestehenden Befugnisse einhergehen, ob die vorhandenen Instrumente überhaupt vollumfänglich eingesetzt werden.*

GESELLSCHAFT
FÜR INFORMATIK

Kontakt

Niklas Sax
Referent Cybersicherheitspolitik
Gesellschaft für Informatik e.V.
E-Mail: niklas.sax@gi.de

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.