



Ausschussdrucksache 21(4)222
vom 30. September 2026

Schriftliche Stellungnahme

der GI Gesellschaft für Informatik, Berlin vom 28.09.2026

zu dem

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

Berlin, 28.09.2026

Stellungnahme

des Fachbereich Sicherheit der Gesellschaft für Informatik e.V. (GI)

zum Gesetzentwurf des Gesetzes zur Stärkung
der Cybersicherheit (Drucksache 21/6585)



Der Fachbereich Sicherheit der Gesellschaft für Informatik e.V. (GI) nimmt zum Entwurf des Gesetzes zur Stärkung der Cybersicherheit in der Fassung der Drucksache 21/6585 vom 22. Juni 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.
- Der Entwurf verlangt von Betreibern kritischer Anlagen, kontinuierlich (laut Gesetzesbegründung minütlich) eine Übermittlung von Verfügbarkeitsindikatoren ihrer maßgeblichen IT-Systeme, -Komponenten und -Prozesse ans BSI über eine direkte Schnittstelle aus ihrem System zur Angriffserkennung. Dies führt einerseits zu einer unnötigen, nicht sachgerechten und damit unverhältnismäßigen Datensammlung bei einer Aufsichtsbehörde und lenkt zugleich Angriffe im Sinne eines Honeypots zielgenau auf die betreffende Schnittstelle, da darüber maßgebliche Information über relevante Angriffsziele übertragen werden. Dieser Schritt gefährdet insoweit sogar die Lage der Cybersicherheit und trägt damit in keinem Fall zu deren Stärkung bei.



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. Angreifer Infrastrukturen 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 §§ 68c–68f 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 weitgehend, sieht jedoch auch hier eine Grenze, die bestehen bleiben sollte. Im Einzelnen:

Schadprogrammerkennung (§ 8 BSIG-neu): 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-neu): 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.

3. Kontinuierliche Ausleitung von Verfügbarkeitsdaten an das BSI

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 dagegen 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. Eine Ausleitung entsprechender Daten aus dem System zur Angriffserkennung heraus entspricht aus Sicht der GI faktisch der Etablierung eines Honeypots. Dieser stellt auf Grund detailliert ablesbarer Informationen im Zielsystem für Angreifende ein besonderes Interesse dar. Bei einer laut Gesetzesbegründung angestrebten minütlichen Ausleitung von Verfügbarkeitsdaten werden zudem zwangsweise Daten in erheblich höheren Detaillierungsgrad übermittelt, als dies bisher im Nachweisverfahren für Betreiber kritischer Anlagen vorgesehen, sowie im Rahmen der Ausleitung von Angriffsindikatoren, zu erwarten ist. Im Gegensatz zu Angriffsindikatoren, für die eingerichtete Systeme zur Angriffserkennung ausdrücklich vorgesehen sind, weshalb in diesem Fall von einer zweckgemäßen Verwendung ausgegangen werden kann, ist der Datenumfang bei Verfügbarkeitsdaten signifikant größer. Beim BSI kann diese unverhältnismäßig große, nicht sachgerecht erweiterte Datenmenge nur mittels KI ausgewertet werden, was ausgerechnet bei einem höchst sensiblen und für die Funktionsfähigkeit der kritischen Anlagen entscheidenden Faktor unkontrollierbare Nebeneffekte auslösen kann, wie aktuelle Berichte über KI-basierte Kollateralschäden nachdrücklich zeigen.

Das bisherige Nachweisverfahren nach § 39 Abs. 1 BSIg weist in der Umsetzung bisher dagegen aus gutem Grund ein geeignetes Abstraktionsniveau bei der mitzuteilenden Beschreibung des Geltungsbereichs auf, wie in Kapitel 3.5 der vom BSI auf Basis von § 39 Abs. 2 BSIg erlassenen Grundsätzlichen Anforderungen im Nachweisverfahren (GAiN) ersichtlich. Eine kritische Anlage besteht oft aus Gründen der Redundanz aus zusammengeschalteten Komponenten, deren jeweilige Verfügbarkeitsdaten wiederum im eingesetzten Monitoringsystem verfolgt werden. Temporäre Nichtverfügbarkeiten



einzelner Komponenten sind dabei vor allem deren ordnungsgemäßer Pflege, sowie mit Updates und Upgrades und der Schließung von Schwachstellen verbundenen, geplanten Nichtverfügbarkeiten geschuldet. Bisher besteht bei den Betreibern kritischer Anlagen i.d.R. bewusst keine Verknüpfung zwischen Monitoringsystem und System zur Angriffserkennung. Sowohl im Monitoringsystem als auch im System zur Angriffserkennung werden wiederum zugehörige Komponenten mit ihren Gerätebezeichnungen und IP-Adressen geführt, damit deren Administration präzise erfolgen kann. Für die Aufsichtsbehörde sind entsprechende Details jedoch von keinem praktischen Interesse, für Angreifer dagegen schon. Damit Verfügbarkeitsindikatoren mit geeigneter Abstraktion und Aussagefähigkeit angezeigt werden könnten, müsste die Zusammenschaltung im System zur Angriffserkennung entsprechend nachgebildet werden, was damit potenziellen Angreifern (inkl. KI-gestützten Kollateral-Angriffen) bei unbefugtem Auslesen zusätzliche Erkenntnisse zur Planung eines zielgerichteten Angriffs liefern würde. Zudem verlangt der Stand der Technik in branchenspezifischen Fällen (z.B. für den Einsatz von Operational Technology nach der IEC 62443) ausdrücklich, dass an höher gelegenen technischen Ebenen Details aus unteren technischen Ebenen eben nicht oder allenfalls nur in stark begrenztem Umfang mitgeteilt werden. Hierzu wird daher in der Praxis meist ein eigenes System zur Angriffserkennung betrieben. Beide miteinander zu verknüpfen, um der neu vorgesehenen Meldepflicht nachkommen zu können, gefährdet insoweit das etablierte Sicherheitskonzept erheblich, ohne dass sich daraus tatsächlich ein nennenswerter Mehrwert für legitime Zwecke ergeben würde. Aus diesen Gründen dürfte die geplante Maßnahme sogar gegen das Übermaßverbot verstoßen.

Empfehlung des Fachbereichs Sicherheit der GI: *Dem äußerst fraglichen, potenziellen Erkenntnisgewinn gegenüber den bestehenden Meldepflichten mittels unverhältnismäßiger Datensammlung steht für die Betreiber kritischer Anlagen ein konkretes strukturelles Sicherheitsrisiko gegenüber. Die GI empfiehlt dem Gesetzgeber daher nachdrücklich, in § 31 Abs. 3 BSIG-neu die Nr. 1 ersatzlos zu streichen. 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 relevante und zielführende 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 jedoch 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

Bernhard C. Witt

Fachexperte für Governance im GI-Fachbereich Sicherheit

E-Mail: bernhard.witt@sits.de

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.