



Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Gesetzentwurf der Bundesregierung

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

Berlin, 05.10.2026
Abt. Innenpolitik | 31, AL3

Sachverständiger: Alexander Poitz, Stellvertretender Bundesvorsitzender

I. - Vorbemerkung

Cyberangriffe stellen eine der zentralen sicherheitspolitischen Herausforderungen dar. Staatliche Einrichtungen, kritische Infrastrukturen, Unternehmen sowie Bürgerinnen und Bürger sind Ziel komplexer und international organisierter Angriffe auf informationstechnische Systeme. Die Sicherheitsbehörden müssen daher über rechtssichere und technisch geeignete Befugnisse verfügen, um solchen Gefahren effektiv begegnen zu können. Die hierfür vorgesehenen Befugnisse müssen hinreichend bestimmt ausgestaltet und auf das erforderliche Maß begrenzt sein. Gerade wegen der hohen Eingriffsintensität sind klare Tatbestandsvoraussetzungen, wirksame Verfahrenssicherungen und eine konsequente Beachtung des Verhältnismäßigkeitsgrundsatzes unverzichtbar.

Insgesamt begrüßt die GdP die Zielsetzung des Gesetzentwurfs, die rechtlichen Rahmenbedingungen für die Cyberabwehr des Bundes zu modernisieren und die Sicherheitsbehörden des Bundes mit spezifischen Eingriffsbefugnissen im Cyberraum auszustatten.

II. - Zum Vorhaben

Die GdP bewertet den Entwurf insgesamt als wichtigen Schritt zur Weiterentwicklung der polizeilichen Cyberabwehr in Deutschland. Positiv hervorzuheben ist insbesondere, dass erstmals spezifische Eingriffsbefugnisse zur Abwehr von Cyberangriffen aufgenommen werden. Dadurch wird den Sicherheitsbehörden ein Mittel zur Verfügung gestellt, das den technischen Besonderheiten von Angriffen auf informationstechnische Systeme besser Rechnung trägt als die bislang vorhandenen klassischen polizeirechtlichen Maßnahmen. Als GdP begrüßen wir, dass den Kolleg:innen, die in der Abwehr und Bekämpfung von Cyberkriminalität eingesetzt sind, zukünftig explizite und belastbare Handlungsinstrumente an die Hand gegeben werden sollen. Die GdP hat bereits in ihrem Impulspapier zur Bundestagswahl 2025¹ angeregt, eine Modernisierung der Cyberabwehrbefugnisse des Bundes für die Abwehr schwerwiegender Cybergefahren vorzunehmen. Der vorliegende Entwurf kommt dieser Anregung nun - in abgewandelter Form - nach.

Besonders zu begrüßen ist aus Sicht der GdP:

- die erstmalige Schaffung cyberspezifischer Befugnisse im BKAG,
- die Aufgabenzuweisung für das BKA im Bereich international koordinierter Cyberabwehr,
- die Verbesserung der Durchsetzbarkeit von Maßnahmen gegenüber Telekommunikationsanbietern und Anbietern digitaler Dienste,
- sowie die rechtliche Absicherung besonders eingriffsintensiver Maßnahmen durch einen Richtervorbehalt bzw. die Möglichkeit bei Gefahr im Verzug zunächst selbst tätig zu werden.

Dass der Gesetzgeber den Weg wählt, die Cyber-Abwehr-Befugnisse auf die bestehenden Gesetzgebungskompetenzen des Bundes gem. Art. 73 f. zu stützen, ist unserer Ansicht nach insgesamt vertretbar.

Er hat zur Folge, dass die allgemeine Gefahrenabwehr im Cyberraum bei den Ländern verbleibt. Letzterer Umstand kann jedoch, so sei angemerkt, aus operativer Sicht problematisch werden,

¹ <https://www.gdp.de/Bundesvorstand/Dokumente/Impulspapiere/GdP-Impulse-zur-BTW-2025.pdf>

da Cyberangriffe häufig keinen klar bestimmbar geographischen Ursprung haben, mehrere Bundesländer gleichzeitig betreffen oder international koordiniert erfolgen. In solchen Lagen besteht weiterhin die Gefahr von Koordinationsproblemen und Zuständigkeitskonflikten zwischen Bund und Ländern, die es gilt, durch enge Kooperation im Sicherheitsverbund zu lösen.

Darüber hinaus verbleiben Zuständigkeiten für die Cyberabwehr weiterhin bei einer Vielzahl von Behörden (Länderpolizeien, Bundespolizei, BKA, BSI). Diese Fragmentierung bindet – aufgrund der Notwendigkeit des Vorhaltens erforderlicher Mehrfachstrukturen und Kooperationsformate – Geld-, Technik- und Personalressourcen, die den beteiligten Behörden durch den Haushaltsgesetzgeber zwingend bereitzustellen sind.

In Ermangelung einer stärkeren Zentralisierung von Cyberabwehrkompetenzen beim Bund, kommt aus praktischer Sicht insbesondere der verbesserten Zusammenarbeit der beteiligten Behörden einschließlich eines verbesserten echtzeitigen Informationsaustauschs eine ebenso herausragende Rolle zu, wie der Verbesserung der Ressourcenausstattung (einschließlich Technik und Personal) bei den betroffenen Behörden. Dabei ist zu berücksichtigen, dass sich Gefahrenabwehr und Strafverfolgung bei Cyberangriffen in der operativen Lage regelmäßig miteinander verknüpft sind. Klare Schnittstellen, belastbare Abstimmungsverfahren und ein rechtssicherer, echtzeitiger Informationsaustausch zwischen den zuständigen Polizeibehörden sind deshalb zwingend erforderlich, um Kompetenzlücken, Doppelstrukturen und Reibungsverluste zu vermeiden.

III. - Im Einzelnen

1. Artikel 1 – Änderung des Bundespolizeigesetzes

Zu Artikel 1 Nr. 2: § 41a BPolG-E – Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik

Mit dem neuen § 41a BPolG-E soll der Bundespolizei erstmals eine ausdrückliche Befugnis eingeräumt werden, im Rahmen ihrer gesetzlichen Aufgaben Cyberangriffe auf informationstechnische Systeme abzuwehren. Hierzu soll sie künftig insbesondere befugt sein, den Betrieb informationstechnischer Systeme zu untersagen, Datenverkehr einzuschränken, zu unterbinden oder umzuleiten, sowie in informationstechnische Systeme einzugreifen, um dort Daten zu erheben, zu löschen oder zu verändern. Die GdP begrüßt grundsätzlich, dass mit § 41a BPolG-E eine ausdrückliche gesetzliche Grundlage für Cyberabwehrmaßnahmen geschaffen werden soll.

Die GdP gibt jedoch zu bedenken, dass der konkrete Anwendungsbereich der Vorschrift im Cyberraum nicht hinreichend klar bestimmt ist. Die Bundespolizei darf die neuen Befugnisse nur im Rahmen ihrer gesetzlichen Aufgaben wahrnehmen. In der Praxis wird häufig unklar sein, wann ein Angriff tatsächlich in den Aufgabenbereich der Bundespolizei fällt und wann andere Behörden insbesondere die Länderpolizeien oder das BKA zuständig sind. Die GdP sieht daher die Gefahr, dass Abgrenzungsprobleme zwischen den Sicherheitsbehörden entstehen können. Zudem muss im Gesetzentwurf klargestellt werden, dass sich die Kompetenz zur Cyberabwehr der Bundespolizei auch zukünftig lediglich im Bereich der Gefahrenabwehr befindet und sich nicht auch auf die Strafverfolgung erstrecken wird.

2. Artikel 2 – Änderung des BSI-Gesetzes

Zur Verbesserung der Zusammenarbeit zwischen beteiligten Behörden sowie zur Verbesserung der Möglichkeiten der polizeilichen Gefahrenabwehr und Strafverfolgung regen wir eine Umwandlung der in § 8 Abs. 6 f. BSI-G festgeschriebenen „Kann-Regelung“ in eine grundsätzliche Datenteilungsregelung, insb. mit den Polizeien des Bundes und der Länder, an.

3. Artikel 3 – Änderung des Bundeskriminalamtgesetzes

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

Mit § 3a BKAG-E soll dem BKA künftig eine besondere Aufgabe im Bereich der Cyberabwehr zugewiesen werden. Danach soll das BKA befugt sein, Cyberangriffe abzuwehren, wenn diese nur im Rahmen international koordinierter Maßnahmen wirksam bekämpft werden können oder aufgrund ihrer Art und ihres Ausmaßes außen- oder sicherheitspolitische Bedeutung für die Bundesrepublik Deutschland haben. Die Vorschrift begründet damit eine spezifische Zuständigkeit des BKA für besonders gelagerte Cybergefahren, ohne eine allgemeine Zuständigkeit des Bundes für die Gefahrenabwehr im Cyberraum zu schaffen.

Die GdP begrüßt ausdrücklich, dass mit § 3a BKAG-E erstmals eine eigenständige Aufgabenzuweisung für das BKA im Bereich der Cyberabwehr geschaffen wird. Gerade bei international koordinierten Cyberangriffen ist eine zentrale bundesweite Zuständigkeit sachgerecht, da solche Lagen regelmäßig eine Zusammenarbeit mit Sicherheitsbehörden anderer Staaten erfordern.

Gleichzeitig bleibt festzustellen, dass der Entwurf bewusst hinter einer umfassenden Zuständigkeitsregelung für den Bund zurückbleibt. Die allgemeine Gefahrenabwehr im Cyberraum verbleibt weiterhin bei den Ländern.

Aus Sicht der GdP stellt dies zwar einen wichtigen ersten Schritt dar, löst jedoch nicht alle strukturellen Herausforderungen. Cyberangriffe lassen sich häufig keinem konkreten Ort zuordnen und betreffen oftmals mehrere Bundesländer gleichzeitig. Die Bearbeitungszuständigkeit richtet sich dann nach dem Tatortprinzip.

In diesem Kontext sei darauf verwiesen, dass Landesbehörden *de lege lata* beim BKA um Unterstützung anfragen können. Bei Annahme des vorliegenden Gesetzentwurfs würde sich eine solche Kompetenz zum Ersuchen um Unterstützung zukünftig *de lege ferenda* auch auf die in Rede stehenden neu zu schaffenden Cyberabwehrbefugnisnormen des BKA erstrecken. Hierfür bedarf es jedoch zwingend des Umstandes, dass auf Landesebene jeweils entsprechende parallele Befugnisnormen existieren bzw. durch die zuständigen Landesgesetzgeber geschaffen werden. In der Praxis können die Länder zwar das BKA ersuchen, benötigen dafür aber selbst die Befugnisse in den jeweiligen Polizeigesetzen. Ergänzend ist sicherzustellen, dass Unterstützung, Informationsübermittlung und die Übernahme oder Koordinierung von Maßnahmen in der dynamischen Cyberlage ohne Zuständigkeitsverluste ineinandergreifen. Nur so lässt sich verhindern, dass die föderale Aufgabenverteilung bei länderübergreifenden oder international vernetzten Angriffen zu einer weiteren Zersplitterung der Verantwortlichkeiten führt.

Vor diesem Hintergrund regt die GdP dringend an, in einem Bund-Länder-Austausch eine Harmonisierung der polizeirechtlichen Cyberabwehrbefugnisse der verschiedenen Ebenen des föderalen Sicherheitssystems herbeizuführen, damit die Polizeibehörden in allen Teilen des Landes gleichermaßen in die Lage versetzt werden, in einem harmonisierten Sicherheitsverbund entsprechende Abwehrmaßnahmen durchführen zu können. Die rechtliche Harmonisierung sollte durch eine zentrale Schnittstelle für die operative Abstimmung flankiert werden. Dort können länderübergreifende Lageinformationen zusammengeführt, Unterstützungsbedarfe frühzeitig erkannt und das Zusammenwirken der zuständigen Stellen verbindlich vorbereitet werden. Dies reduziert Verzögerungen und Mehrfachstrukturen, ohne die Entscheidungskompetenz der jeweils zuständigen Behörde zu verlagern. Hierfür böte sich eine Weiterentwicklung des Nationalen Cyber-Abwehrzentrums an.

Zu Artikel 3: Abschnitt 8a – Cyberabwehrbefugnisse (§§ 68a ff. BKAG-E)

Mit dem neuen Abschnitt 8a BKAG sollen dem BKA erstmals spezifische Eingriffsbefugnisse zur aktiven Cyberabwehr eingeräumt werden. Hierzu gehören insbesondere Befugnisse, informationstechnische Systeme zu deaktivieren oder deren Betrieb zu untersagen, Datenverkehr zu blockieren, einzuschränken oder umzuleiten, sowie in informationstechnische Systeme einzugreifen, um dort Daten zu erheben, zu verändern oder zu löschen. Diese Maßnahmen sollen insbesondere eingesetzt werden können, um Angriffsinfrastrukturen wie Botnetze zu neutralisieren, schädlichen Datenverkehr zu unterbinden oder Command-and-Control-Server zu kontrollieren.

Die GdP begrüßt die Einführung eigenständiger Befugnisse für Cyberabwehrmaßnahmen im BKAG ausdrücklich. Die vorgesehenen Regelungen tragen den technischen Besonderheiten moderner Cyberangriffe Rechnung und schaffen erstmals ein rechtlich klar geregeltes Instrumentarium zur aktiven Abwehr solcher Angriffe.

Ebenfalls positiv bewertet die GdP, dass die Cyberbefugnisse nicht ausschließlich an die neue Aufgabe nach § 3a BKAG gebunden sind, sondern auch im Rahmen anderer Aufgaben des BKA etwa der Terrorismusabwehr eingesetzt werden können.

§ 68e BKAG-E – Eingriffe in private informationstechnische Systeme

Der Entwurf sieht vor, dass besonders eingriffsintensive Maßnahmen insbesondere Eingriffe in private informationstechnische Systeme ohne Einwilligung des Betroffenen grundsätzlich nur auf Grundlage einer gerichtlichen Anordnung erfolgen dürfen.

Die GdP hält diese Regelung für einen wichtigen Beitrag zur rechtlichen Absicherung der vorgesehenen Maßnahmen. Der vorgesehene Richtervorbehalt trägt dazu bei, die verfassungsrechtlichen Anforderungen an solche Eingriffe zu wahren und zugleich die Rechtssicherheit für die handelnden Behörden zu erhöhen, da auch bei Gefahr im Verzug die Handlungsfähigkeit erhalten bleibt.

§ 68f BKAG-E – Offenbarungsverbot

Der Entwurf sieht ferner vor, dass das BKA gegenüber beteiligten Diensteanbietern ein Offenbarungsverbot anordnen kann, wenn die Bekanntgabe einer Maßnahme den Erfolg der Gefahrenabwehr gefährden würde.

Die GdP unterstützt die Einführung eines solchen Offenbarungsverbots. Die Möglichkeit, entsprechende Maßnahmen zunächst verdeckt durchzuführen, kann entscheidend für den Erfolg von Cyberabwehrmaßnahmen sein.

Zu Artikel 3 Nr. 14: § 87a BKAG-E – Bußgeldvorschriften

Mit dem neuen § 87a BKAG sollen Bußgeldvorschriften eingeführt werden, um die Durchsetzbarkeit der vorgesehenen Cyberabwehrbefugnisse des BKA zu gewährleisten. Künftig soll das BKA zur Abwehr von Gefahren für die Sicherheit der Informationstechnik auch Dritte insbesondere Telekommunikationsanbieter oder Anbieter digitaler Dienste zur Mitwirkung verpflichten können. Zur Sicherstellung der praktischen Wirksamkeit dieser Maßnahmen soll eine Bußgeldbewehrung für Fälle der rechtswidrigen Nichtmitwirkung geschaffen werden. Darüber hinaus soll auch ein Verstoß gegen ein nach § 68f BKAG angeordnetes Offenbarungsverbot als Ordnungswidrigkeit sanktioniert werden können.

Die GdP begrüßt die Einführung entsprechender Bußgeldtatbestände. Ohne eine rechtlich durchsetzbare Verpflichtung zur Mitwirkung besteht die Gefahr, dass notwendige Maßnahmen zur Gefahrenabwehr nicht oder nur verzögert umgesetzt werden können.

IV. - Des Weiteren

Vor dem Hintergrund des beschriebenen grundsätzlich bestehenbleibenden Nebeneinanders behördlicher sowie föderal verteilter Zuständigkeiten zur Cyberabwehr regen wir eine Evaluierungsvorgabe des Gesetzes gerade auch mit diesem Schwerpunkt an, damit bei Auffälligkeiten hier nachjustiert werden. Hier wäre dann auch die Notwendigkeit einer Grundgesetzänderung mit dem Ziel der Ermöglichung einer stärkeren Zentralisierung der Kompetenzen im in Rede stehenden Deliktbereich beim Bund zu prüfen. Die Evaluation sollte insbesondere erfassen, ob die gesetzlich vorgesehenen Zuständigkeiten, Koordinierungswege und Informationsflüsse in der Praxis ein wirksames, rechtssicheres und verhältnismäßiges Zusammenwirken von Gefahrenabwehr und Strafverfolgung gewährleisten.