Bund Deutscher Kriminalbeamter

BDK |Wollankstraße 135|D-13187Berlin

An das Bundesministerium des Innern
und für Heimat
Alt-Moabit 140
10557 Berlin

Per Mail: CI1@bmi.bund.de

Bundesvorsitzender

Ansprechpartner/in: Dirk Peglow
Funktion: Bundesvorsitzender

E-Mail: dirk.peglow@bdk.de
Telefon: +49 30 2463045-0

Datum: 17.03.2026

Stellungnahme des Bund Deutscher Kriminalbeamter e.V. (BDK) zum Referentenentwurf des Bundesministeriums des Innern (BMI) für ein Gesetz zur Stärkung der Cybersicherheit BMI, CI1.20017/20#2

Der Bund Deutscher Kriminalbeamter bedankt sich für die Möglichkeit, zu dem vorliegenden Referentenentwurf zur Stärkung der Cyberabwehr Stellung zu nehmen.

1. Ausgangslage und Einordnung

Cyberangriffe stellen mittlerweile eine der zentralen sicherheitspolitischen Herausforderungen für Staat, Wirtschaft und Gesellschaft dar. Staatliche Stellen, Unternehmen sowie Bürgerinnen und Bürger werden zunehmend Ziel komplexer digitaler Angriffe, die erhebliche wirtschaftliche Schäden verursachen und im Extremfall auch die Funktionsfähigkeit staatlicher Strukturen beeinträchtigen können. Tätergruppen agieren dabei häufig international, arbeitsteilig und hochgradig professionalisiert. Große Ransomwarekampagnen, Angriffe auf kritische Infrastrukturen oder koordinierte Angriffe auf staatliche Systeme zeigen, dass digitale Angriffe innerhalb kürzester Zeit erhebliche Schäden verursachen können.

Moderne Cyberangriffe folgen häufig arbeitsteiligen Strukturen. Schadsoftware wird von spezialisierten Gruppen entwickelt, während andere Akteure Botnetze betreiben, kompromittierte Systeme steuern oder technische Dienstleistungen im Bereich Infrastruktur und Geldwäsche bereitstellen. Angriffe erfolgen über weltweit verteilte Serverstrukturen, kompromittierte Systeme oder komplexe Botnetze und überschreiten regelmäßig nationale Grenzen.

Vor diesem Hintergrund begrüßt der Bund Deutscher Kriminalbeamter grundsätzlich, dass der Gesetzgeber die rechtlichen Grundlagen zur Abwehr schwerwiegender Cyberangriffe weiterentwickelt.

Positiv hervorzuheben ist insbesondere, dass der Referentenentwurf den Sicherheitsbehörden des Bundes erstmals ausdrücklich Befugnisse zur präventiven Unterbindung von Cyberangriffen einräumt und damit auf die veränderte Bedrohungslage reagiert.

2. Bewertung des Referentenentwurfs

2.1 Notwendigkeit einer aktiven Cyberabwehr
Der Referentenentwurf verfolgt das Ziel, schwerwiegende Cyberangriffe künftig nicht mehr ausschließlich im Nachhinein strafrechtlich aufzuklären, sondern sie bereits im laufenden Angriff technisch zu unterbinden. Hierfür sollen dem Bundeskriminalamt und der Bundespolizei neue Befugnisse eingeräumt werden, die beispielsweise die Umleitung oder Unterbindung von Datenverkehr, die Stilllegung informationstechnischer Systeme oder Eingriffe in digitale Infrastrukturen ermöglichen.

Dieser Ansatz ist aus kriminalfachlicher Sicht nachvollziehbar und grundsätzlich zu begrüßen. Angesichts der Geschwindigkeit und Komplexität moderner Cyberangriffe ist eine rein reaktive Strafverfolgung nicht ausreichend, um gravierende Schäden zu verhindern.

2.2 Verzahnung von Gefahrenabwehr und Strafverfolgung
Bei der Bekämpfung schwerer Cyberangriffe ist zudem zu berücksichtigen, dass Gefahrenabwehr und Strafverfolgung im Cyberraum eng miteinander verzahnt sind. Technische Maßnahmen zur Unterbindung laufender Angriffe – etwa die Analyse von Schadsoftware, die Identifizierung kompromittierter Systeme oder die Übernahme krimineller Infrastruktur – liefern regelmäßig zugleich wesentliche Erkenntnisse für spätere strafrechtliche Ermittlungen.

Umgekehrt entstehen operative Ansätze zur Unterbindung von Angriffen häufig erst im Rahmen strafrechtlicher Ermittlungen. Erkenntnisse aus Ermittlungen können Hinweise auf laufende oder unmittelbar bevorstehende Cyberangriffe liefern und ermöglichen so präventive Maßnahmen zur Gefahrenabwehr.

Daher erscheint es aus unserer Sicht dringend geboten, dass Gefahrenabwehr und Strafverfolgung im Bereich schwerer Cyberangriffe eng miteinander verzahnt und organisatorisch möglichst aus einer Hand wahrgenommen werden.

3. Redundante Zuständigkeitsstruktur

Der oben beschriebenen Verzahnung von Gefahrenabwehr und Strafverfolgung folgt der vorliegende Entwurf jedoch nicht in vollem Umfang. Stattdessen wird vorgesehen, entsprechende Cyberabwehrbefugnisse sowohl dem Bundeskriminalamt als auch der Bundespolizei (bei unterschiedlichen Fallkonstellationen) einzuräumen. Gleichzeitig wird das Bundesamt für Sicherheit

in der Informationstechnik weiter gestärkt und soll insbesondere im Bereich der Detektion und Analyse von Cyberangriffen eine zentrale Rolle einnehmen.

Diese Aufgabenteilung ist grundsätzlich nachvollziehbar. Gleichwohl entsteht durch die parallele Ausstattung mehrerer Behörden mit weitreichenden Eingriffsbefugnissen die Gefahr unklarer Zuständigkeitsstrukturen. Cyberangriffe entwickeln sich häufig sehr dynamisch und erfordern schnelle technische Entscheidungen. In solchen Situationen können unklare Zuständigkeiten oder parallele Kompetenzen zu Koordinationsproblemen und zeitlichen Verzögerungen führen.

Die im Referentenentwurf vorgesehenen Maßnahmen ermöglichen teilweise tiefgreifende Eingriffe in informationstechnische Systeme. Dazu gehören unter anderem Maßnahmen zur Umleitung oder Unterbindung von Datenverkehr sowie technische Eingriffe in IT-Systeme zur Veränderung oder Löschung von Daten.

4. Notwendigkeit einer klar definierten Bundeskompetenz

Die Gefahrenabwehr ist nach der Systematik des Grundgesetzes grundsätzlich Aufgabe der Länderpolizeien. Der Bund kann eigene Gefahrenabwehrbefugnisse nur wahrnehmen, wenn hierfür eine ausdrückliche verfassungsrechtliche Kompetenz besteht.

Eine solche Kompetenz existiert für das BKA beispielsweise im Bereich der Terrorismusabwehr. Auf dieser Grundlage wurde mit § 5 BKAG eine Regelung geschaffen, die es dem Bundeskriminalamt ermöglicht, unter bestimmten Voraussetzungen eigenständig Gefahren des internationalen Terrorismus abzuwehren. Für schwere Cyberangriffe ohne terroristische Motivlage existiert eine vergleichbare verfassungsrechtliche Grundlage bislang nicht.

Aus kriminalfachlicher Sicht wäre eine Regelung nach dem Vorbild des § 5 BKAG jedoch langfristig sachgerecht und notwendig. Schwere Cyberangriffe sind regelmäßig länderübergreifend organisiert, international vernetzt und betreffen häufig kritische Infrastrukturen oder zentrale staatliche Funktionen. Eine klar definierte bundesweite Zuständigkeit für die Abwehr von Cyberangriffen könnte daher zu einer deutlich effizienteren und schnelleren Gefahrenabwehr beitragen.

Der vorliegende Gesetzentwurf stellt vor diesem Hintergrund einen pragmatischen Schritt innerhalb der bestehenden verfassungsrechtlichen Grenzen dar. Er kann jedoch eine langfristige Diskussion über eine klarere verfassungsrechtliche Grundlage für die Cyberabwehr nicht ersetzen

5. Koordinierung der Cyberabwehr – Weiterentwicklung des Cyber-Abwehrzentrums

Unabhängig von der konkreten gesetzlichen Zuständigkeitsregelung ist entscheidend, dass vorhandene Fähigkeiten der Sicherheitsbehörden effektiv zusammengeführt werden.

Sowohl das Bundeskriminalamt als auch die Bundespolizei verfügen über spezialisierte technische Kompetenzen im Bereich der Cyberabwehr. Gleichzeitig kommt dem Bundesamt für Sicherheit in der Informationstechnik eine zentrale Rolle bei der Erkennung und Analyse von Cyberangriffen zu. Eine effektive Cyberabwehr erfordert daher eine enge und dauerhafte Zusammenarbeit dieser Akteure.

Vor diesem Hintergrund sollte geprüft werden, das Nationale Cyber-Abwehrzentrum zu einem operativen Lage- und Koordinierungszentrum weiterzuentwickeln.

Ein solcher Ausbau könnte insbesondere folgende Elemente umfassen:

- Einrichtung eines ständig besetzten 24/7 Cyberlagezentrums
- Bildung gemeinsamer Einsatzteams aus BKA, Bundespolizei und weiteren beteiligten Behörden
- Entwicklung klarer Prozesse und Einsatzabläufe für Cyberabwehrmaßnahmen
- Einrichtung einer gemeinsamen technischen und juristischen Einsatzunterstützung

Durch eine solche Struktur könnten operative Maßnahmen koordiniert vorbereitet und umgesetzt werden, ohne dass zunächst Zuständigkeitsfragen zwischen Behörden geklärt werden müssen.

6. Auswirkungen auf die Polizeigesetze der Länder

Mit der Einführung neuer Cyberabwehrbefugnisse auf Bundesebene stellt sich zugleich die Frage nach der zukünftigen Rolle der Polizeien der Länder.

Cyberangriffe betreffen regelmäßig nicht nur Bundesinstitutionen oder kritische Infrastrukturen von nationaler Bedeutung, sondern ebenso Unternehmen, öffentliche Einrichtungen und Infrastrukturen in den Ländern. In vielen Polizeigesetzen der Länder bestehen bislang keine vergleichbaren Eingriffsbefugnisse zur aktiven Unterbindung schwerer Cyberangriffe.

Aus polizeipraktischer Sicht sollte daher geprüft werden, ob auch auf Ebene der Länder entsprechende Anpassungen erforderlich sind. Eine wirksame Sicherheitsarchitektur im Cyberraum erfordert eine abgestimmte Weiterentwicklung der gesetzlichen Grundlagen auf Bundes- und Landesebene.

Bund Deutscher Kriminalbeamter

7. Schlussbemerkung

Der Bund Deutscher Kriminalbeamter unterstützt das Ziel des Gesetzgebers, die rechtlichen Grundlagen für eine wirksame Cyberabwehr weiterzuentwickeln. Der Referentenentwurf stellt einen wichtigen Schritt dar, da er erstmals aktive Maßnahmen zur Unterbindung schwerwiegender Cyberangriffe ermöglicht.

Gleichzeitig bleibt festzuhalten, dass der Entwurf keine eindeutig strukturierte Zuständigkeitsordnung schafft. Langfristig wäre aus kriminalfachlicher Sicht eine klarere Zuständigkeit des Bundes – etwa nach dem Vorbild des § 5 BKAG – eine sachgerechtere Lösung.

Bis dahin sollte der Gesetzgeber sicherstellen, dass vorhandene Fähigkeiten der Sicherheitsbehörden effektiv gebündelt werden. Ein Ausbau des Cyber-Abwehrzentrums zu einem operativen Koordinierungs- und Lagezentrum könnte hierfür einen praktikablen Weg darstellen.

Mit freundlichen Grüßen

Dirk Peglow
Bundesvorsitzender

Marina Hackenbroch
Stellvertretende Bundesvorsitzende