Bund Deutscher Kriminalbeamter

BDK zur Reform des Nachrichtendienstrechts: Stärkere Nachrichtendienste brauchen klare Grenzen

13.08.2026

Der Bund Deutscher Kriminalbeamter (BDK) begrüßt grundsätzlich die geplante Stärkung der Nachrichtendienste. Angesichts wachsender Gefahren durch Spionage, Sabotage, Extremismus und staatlich gesteuerte Cyberangriffe ist es notwendig, Bundesnachrichtendienst und Bundesamt für Verfassungsschutz rechtlich und technisch so aufzustellen, dass sie ihren Aufgaben auch unter veränderten Bedrohungsbedingungen wirksam nachkommen können.

Gleichzeitig sieht der BDK im weiteren Gesetzgebungsverfahren Klärungsbedarf – insbesondere dort, wo sich die Aufgaben und Befugnisse von Nachrichtendiensten, Polizei und Justiz überschneiden.

> „Ich halte es für richtig, unsere Nachrichtendienste angesichts der aktuellen Bedrohungslage zu stärken. Aber dort, wo aus Nachrichtengewinnung konkrete Gefahrenabwehr wird, müssen Zuständigkeit und Verantwortung eindeutig geregelt sein“, erklärt Dirk Peglow, Bundesvorsitzender des Bund Deutscher Kriminalbeamter.

Verfassungsschutz darf nicht zur zweiten Gefahrenabwehrbehörde werden

Kritisch sieht der BDK insbesondere operative Befugnisse des Bundesamtes für Verfassungsschutz im Inland. Wenn ein Nachrichtendienst künftig IT-Systeme beeinträchtigen, Daten verändern oder löschen oder Tatmittel unbrauchbar machen kann, berührt das unmittelbar Bereiche der polizeilichen Gefahrenabwehr und Strafverfolgung.

> „Für mich ist die entscheidende Frage nicht, ob der Verfassungsschutz im Ausnahmefall operativ handeln können muss. Entscheidend ist, wo wir die Grenze ziehen. Die Gefahrenabwehr im Inland ist und bleibt grundsätzlich Aufgabe der Polizei. Wir dürfen nicht durch die Hintertür eine zweite Gefahrenabwehrbehörde neben der Polizei schaffen.“

Für außergewöhnliche Gefahrenlagen kann es eng begrenzte Ausnahmen geben. Dann müssen jedoch Voraussetzungen, Dokumentation und die Übergabe an die zuständige Polizeibehörde eindeutig geregelt sein.

> „Wenn Sekunden oder Minuten entscheiden, wird niemand verlangen, dass eine Behörde erst Zuständigkeitsfragen klärt. Aber aus einer Ausnahme darf keine neue Regelzuständigkeit entstehen.“

Cyberabwehr braucht klare Führung

Besonders deutlich werden mögliche Überschneidungen bei schweren Cyberangriffen. Nachrichtendienste, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundeskriminalamt (BKA) und Polizeibehörden der Länder können hier gleichzeitig über relevante Erkenntnisse und Fähigkeiten verfügen.

Das BSI bringt seine technische Expertise ein, die Nachrichtendienste ihre Erkenntnisse aus dem In- und Ausland.

> „Cyberangriffe interessieren sich nicht dafür, welche Behörde nach welchem Gesetz zuständig ist. Genau deshalb muss der Staat diese Frage vorher geklärt haben. Am Ende muss einer den Hut aufhaben. Wir brauchen eine belastbare Kette von der Erkennung über die Abwehr bis zur Strafverfolgung.“

Dabei geht es nicht darum, die originären Ermittlungszuständigkeiten der Länder auf das BKA zu verlagern. Bei schweren länderübergreifenden oder internationalen Cyberangriffen muss das BKA aber seine Zentralstellenfunktion wirksam wahrnehmen können.

Aktive Abwehr darf Strafverfolgung nicht erschweren

Ein Eingriff in ein von Angreifern genutztes IT-System kann einen laufenden Angriff stoppen. Gleichzeitig besteht die Gefahr, digitale Spuren zu verändern, Tatverdächtige zu warnen oder laufende nationale und internationale Ermittlungen zu gefährden.

Der BDK fordert deshalb, Polizei und Staatsanwaltschaft frühzeitig einzubeziehen, sobald konkrete Anhaltspunkte für Straftaten bestehen. Ebenso müssen die forensische Sicherung und Dokumentation digitaler Beweise verbindlich geregelt werden.

> „Wir dürfen nicht nur darüber reden, wie wir einen Cyberangriff möglichst schnell stoppen. Wir müssen genauso darüber reden, was danach kommt. Wenn wir einen Angriff erfolgreich abwehren, dabei aber sämtliche Spuren vernichten und die Täter anschließend nicht mehr identifizieren können, haben wir nur die Hälfte unserer Arbeit gemacht.“

Gerade bei staatlich gesteuerten Cyberangriffen und international agierenden Tätergruppen muss zudem berücksichtigt werden, dass Eingriffe in technische Infrastrukturen auch laufende Ermittlungen anderer Behörden oder Staaten berühren können.

> Peglow abschließend: „Deutschland braucht leistungsfähige Nachrichtendienste und eine leistungsfähige Polizei. Was wir nicht brauchen, sind mehrere Behörden mit ähnlichen operativen Befugnissen und hinterher die Diskussion darüber, wer eigentlich zuständig gewesen wäre.“

Schlagwörter
Bund Verfassungsschutz Cybercrime
diesen Inhalt herunterladen: PDF