Nr. 569 | August 2026

Analysen & Argumente

KONRAD ADENAUER STIFTUNG

Zeitenwende für das Trennungsgebot!

Ansätze, um Polizei und Nachrichtendienste vor die Lage zu bringen

Franca König, Sandra Lukosek, Till Nierhoff

- Hybride Bedrohungen überschreiten klassische Zuständigkeiten und stellen das informationelle Trennungsprinzip zwischen Polizei und Nachrichtendiensten vor neue Herausforderungen.
- Das Trennungsgebot bleibt eine wichtige rechtsstaatliche Leitplanke, verhindert jedoch keine engere Zusammenarbeit zwischen Polizei und Nachrichtendiensten und muss an die Anforderungen moderner, hybrider Bedrohungslagen angepasst werden.
- Informationsaustausch über gemeinsame Zentren reicht nicht mehr aus: Sicherheitsrelevante Erkenntnisse müssen schneller zusammengeführt, analysiert und bewertet werden.
- Die sicherheitspolitische Zeitenwende erfordert nicht nur erweiterte Befugnisse, sondern vor allem eine moderne Organisation der behördenübergreifenden Zusammenarbeit und Fortentwicklung der deutschen Sicherheitsarchitektur.
- Behördenübergreifende Verfahren zur frühzeitigen Erkennung hybrider Verdachtsfälle sollten geschaffen und praxistaugliche Übermittlungsschwellen festgelegt werden.

1. Hybride Bedrohungen als neue sicherheitspolitische Realität

Eine neue sicherheitspolitische Lage

Die sicherheitspolitische Lage Deutschlands hat sich grundlegend verändert. Kriege, geopolitische Spannungen und internationale Krisen lassen äußere und innere Bedrohungen zunehmend ineinander übergehen. Terrorismus, Spionage, Sabotage, Cyberangriffe und ausländische Einflussnahme überschreiten Zuständigkeiten und stellen die Trennung zwischen Nachrichtendiensten und Polizei vermehrt infrage.

Hybride Bedrohungen prägen die Arbeit der Sicherheitsbehörden seit Jahren. Beispiele sind der Einsatz einer russischen Schattenflotte in der Ostsee, unautorisierte Drohnen über militärischen Anlagen und Flughäfen, Straftaten durch Wegwerf- bzw. Low-Level-Agenten im Auftrag ausländischer Nachrichtendienste, die Nutzung krimineller und terroristischer Netzwerke und physische Sabotage gegen kritische Infrastrukturen sowie Desinformationskampagnen. Diese Phänomene überschreiten regelmäßig die Zuständigkeiten einzelner Behörden. Die informationelle Trennung zwischen Nachrichtendiensten und Polizei ist vor diesem Hintergrund nicht länger zeitgemäß. Sie verhindert die notwendige Zusammenführung sicherheitsrelevanter Erkenntnisse.

An der Schnittstelle zwischen äußerer und innerer Sicherheit stehen – neben den Strafverfolgungsbehörden – die Nachrichtendienste, also der Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV)[1] und das Bundesamt für den Militärischen Abschirmdienst (BAMAD). Gleichwohl ist eine sicherheitspolitische Zeitenwende in diesem Bereich bislang ausgeblieben, weswegen die Nachrichtendienste rechtlich wie organisatorisch nur begrenzt auf die aktuellen Bedrohungen ausgerichtet sind.

Mit dem Referentenentwurf zur Änderung des Nachrichtendienstrechts (Stand: 06. Juli 2026) plant die Bundesregierung die größte Reform seit Gründung der Bundesrepublik. Positiv hervorzuheben sind die Zusammenarbeitspflicht im Verfassungsschutzverbund, einschließlich der gegenseitigen Unterstützungs- und Hilfeleistungen, die Erweiterung der Übermittlungsschwellen und Intensivierung des Informationsaustauschs sowie gemeinsame Analysemöglichkeiten. Der Entwurf zielt jedoch insbesondere auf eine stärkere Operationalisierung der Dienste und verändert die bestehende, organisatorisch zersplitterte Sicherheitsarchitektur nicht.

Dabei hat das Trennungsgebot – also die umfassende Trennung von Nachrichtendiensten und Polizeien – institutionelle Doppelstrukturen begünstigt. Zwar stellt es kein Kooperationsverbot dar, es gilt jedoch ein informationelles Trennungsprinzip zwischen den Behörden. Hybride Bedrohungen zeigen den bestehenden Strukturen zusätzlich Grenzen auf. Soll die Arbeit der Nachrichtendienste effizienter werden, bedürfte es hier ebenfalls Änderungen. Trotz wichtiger Verbesserungen bleibt das informelle Trennungsprinzip unangetastet und verhindert einen strukturellen Durchbruch bei der Fortentwicklung der deutschen Sicherheitsarchitektur. Hier setzt dieses Papier an.

2. Fallbeispiel: Wie informationelle Trennung Sicherheitslücken schafft

Die Hürden informeller Trennung

Die Defizite der gegenwärtigen Sicherheitsarchitektur zeigen sich insbesondere dort, wo sicherheitsrelevante Einzelinformationen zwar vorhanden sind, aufgrund informationeller Trennung jedoch nicht rechtzeitig zu einem gemeinsamen Lagebild verdichtet und damit nicht berücksichtigt werden. Dies verdeutlicht der folgende hypothetische Fall:

Ein chinesischer Staatsangehöriger wird von einer Polizeistreife kontrolliert, nachdem er eine handelsübliche Kameradrohne nahe einer sicherheitsrelevanten Bundesliegenschaft betrieben hat. Er gibt an, als Technikstudent mit einem Touristenvisum nach Deutschland eingereist zu sein und sich für Stadtarchitektur zu interessieren. Die Polizei bewertet den Vorfall als möglichen luftverkehrsrechtlichen Verstoß; konkrete Anhaltspunkte für eine sicherheitsrelevante Motivation liegen nicht vor. Der polizeiliche Staatsschutz wird nicht beteiligt.

Erst nachträglich wird bekannt, dass der BND bereits Erkenntnisse über die Person besaß. Diese betrafen Verbindungen zu einer staatlichen chinesischen Forschungseinrichtung für militärische Drohnentechnologie sowie Besuche europäischer Technologieunternehmen und einer Fachmesse für autonome Systeme. Mangels rechtzeitiger Zusammenführung dieser Erkenntnisse war keine umfassende Risikobewertung möglich.

Der hypothetische Fall verdeutlicht das strukturelle Defizit der gegenwärtigen Sicherheitsarchitektur: Polizei, BfV und BND verfügen jeweils über unterschiedliche, komplementäre Informationen, die aufgrund ihrer gesetzlichen Zuständigkeiten getrennt bleiben. Eine institutionalisierte Stelle zur behördenübergreifenden Verdichtung dieser Erkenntnisse existiert nicht. Dadurch können sicherheitsrelevante Sachverhalte trotz bereits vorhandener Einzelinformationen unerkannt bleiben.

3. Das Trennungsgebot als Strukturprinzip

Das Trennungsgebot gehört seit Gründung der Bundesrepublik zu den grundlegenden Strukturprinzipien der deutschen Sicherheitsarchitektur. Es soll verhindern, dass nachrichtendienstliche Informationsgewinnung und polizeiliche Zwangsbefugnisse zusammenfallen und gilt als Ausdruck der historischen Erfahrungen mit den Sicherheitsapparaten des Nationalsozialismus. Ausgangspunkt war der Polizeibrief der Alliierten von 1949, der einen (Inlands-)Nachrichtendienst ohne polizeiliche Befugnisse vorsah[2] und damit die institutionelle Trennung von Nachrichtendiensten und Polizei begründete.[3]

Die vier Dimensionen des Trennungsgebotes

Das Trennungsgebot umfasst mindestens vier Dimensionen:[4] die organisatorische, personelle, funktionelle sowie die informationelle Trennung. Gleichwohl ist das Trennungsgebot kein Kooperationsverbot. Nachrichtendienste und Polizei arbeiten sowohl im Rahmen gesetzlicher Übermittlungsvorschriften als auch in institutionalisierten Kooperationsformaten bzw. -zentren zusammen. Dabei verbleiben Personal, Zuständigkeiten und Entscheidungsbefugnisse bei den jeweiligen Stammbehörden.[5]

In der politischen und juristischen Debatte wird das Trennungsgebot unterschiedlich bewertet. Während seine Befürworter und Befürworterinnen darin eine unverzichtbare Konsequenz aus der historischen Erfahrung mit Machtkonzentration in Sicherheitsbehörden sehen und ihm teilweise Verfassungsrang zuschreiben, verweisen Kritiker und Kritikerinnen auf Doppelstrukturen sowie Koordinationsdefizite bei der Bekämpfung komplexer und hybrider Bedrohungslagen.

Tatsächlich ist das Trennungsgebot weder ausdrücklich im Grundgesetz normiert noch hat das Bundesverfassungsgericht ihm bislang Verfassungsrang zuerkannt.[6] Seine einfachgesetzliche Ausprägung findet es in den Nachrichtendienstgesetzen des Bundes und der Länder.[7] Maßgeblich ist zudem das Urteil des Bundesverfassungsgerichts zur Antiterrordatei. Das Gericht leitete darin das informationelle Trennungsprinzip aus dem Grundrecht auf informationelle Selbstbestimmung ab. Danach sind der behördenübergreifende Austausch zwischen Nachrichtendiensten und Polizei sowie die gemeinsame Nutzung von Daten wegen ihres hohen Grundrechtseingriffs nur ausnahmsweise zulässig.[8] Hintergrund hierfür ist, dass Nachrichtendienste personenbezogene Daten bereits unter geringeren Voraussetzungen als Polizeibehörden erheben dürfen; eine operative Nutzung durch die Polizei kommt daher grundsätzlich nur zum Schutz besonders gewichtiger Rechtsgüter in Betracht.

Die Entscheidung unterstreicht die grundrechtliche Bedeutung des informationellen Trennungsprinzips, zeigt zugleich aber die verfassungsrechtlichen Voraussetzungen zulässiger Kooperation auf. Angesichts moderner Bedrohungslagen wie Cyberangriffen und Sabotagen gilt es, diesen Rechtsrahmen fortzuentwickeln, um die Handlungsfähigkeit der Sicherheitsbehörden dauerhaft zu gewährleisten.

4. Vom Informationsaustausch zur gemeinsamen Risikobewertung

Hybride Bedrohungen entstehen häufig an den Schnittstellen zwischen innerer und äußerer Sicherheit sowie zwischen polizeilicher Gefahrenabwehr und nachrichtendienstlicher Aufklärung. Während Gefahren zunehmend multidimensional auftreten, bleiben die Sicherheitsbehörden entlang starrer Zuständigkeiten organisiert und können diese Entwicklungen nur unzureichend abbilden. Das zentrale Defizit liegt dabei weniger im Fehlen sicherheitsrelevanter Informationen als in deren rechtzeitiger Auswertung, Übermittlung und Zusammenführung.

Frühzeitige Erkennung nachrichtendienstlicher Relevanz

Informationsaustausch durch standardisierte Verfahren

Polizeibehörden treffen regelmäßig auf Personen oder Sachverhalte, die den Nachrichtendiensten bereits bekannt sind. Um sicherheitsrelevante Erkenntnisse festzustellen, bedarf es hierfür nicht zwingend einer Übermittlung nachrichtendienstlicher Informationen. Bereits ein technisch standardisiertes Abfrageverfahren (Hit-/No-Hit) könnte Polizeibediensteten signalisieren, dass bereits Informationen an anderer Stelle vorliegen. Die zuständige Sicherheitsbehörde könnte daraufhin weitere Prüfungen oder Folgemaßnahmen veranlassen. Gerade bei Personen mit Auslandsbezügen ließen sich so bestehende Informationslücken frühzeitig erkennen und schließen.

Ebenso wichtig ist der Rückfluss polizeilicher Erkenntnisse an die Nachrichtendienste. Hierfür bedarf es neben einer stärkeren Sensibilisierung der Einsatzkräfte für Anhaltspunkte von Spionage, Sabotage, transnationaler Repressionen, Mord- und Entführungskomplotten und ausländischer Einflussnahme vor allem einheitlicher Erfassungs- bzw. Prüfmerkmale sowie standardisierter Meldewege. Denkbar wäre beispielsweise die Einführung einer Kategorie „Hybride Bedrohungen“ in polizeilichen Vorgangsbearbeitungssystemen, um entsprechende Sachverhalte und Verdachtsfälle systematisch zu kennzeichnen und lagebildfähig aufzubereiten.

Der Referentenentwurf erweitert die Übermittlungspflichten sicherheitsrelevanter Erkenntnisse an das BfV durch BND, Polizeien und weitere öffentliche Stellen und ermöglicht sowohl anlassbezogene Übermittlungen auf Ersuchen als auch Spontanübermittlungen bei tatsächlichen Anhaltspunkten für Bedrohungen (§ 10 BVerfSchG-E). Während das BAMAD in das gemeinsame nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden einbezogen wird (§ 6 BVerfSchG-E), bleibt der BND weiterhin außerhalb dieses Systems und wird über eigenständige Übermittlungspflichten eingebunden (§ 10 Abs. 4 Nr. 1, Abs. 7 Nr. 1 BVerfSchG-E). Parallel schafft der Entwurf mit § 10 BNDG-E eine umfassende Grundlage für die Datenübermittlung zwischen BND und Polizeien sowie weiteren inländischen öffentlichen Stellen. Darüber hinaus werden BfV und BND erstmals ausdrücklich ermächtigt, im polizeilichen Informationsverbund Ausschreibungen zur verdeckten Kontrolle von Personen und Gegenständen zu veranlassen (§ 10 Abs. 3 BVerfSchG-E; § 11 Abs 3 BNDG-E).

Gleichwohl sieht der Entwurf weder einen standardisierten Echtzeitabgleich zwischen polizeilichen und nachrichtendienstlichen Informationssystemen vor noch Grundlagen für eine einheitliche Prüfung und Erfassung hybrider Verdachtsfälle. Wenngleich er die „Fortbildung in speziellen Arbeitsbereichen“ innerhalb des Verfassungsschutzverbundes anvisiert (§ 5 BVerfSchG-E), sieht er keine Regelungen zur Sensibilisierung von polizeilichen Einsatzkräften oder anderer öffentlicher Stellen vor. Insoweit müssen weitere Reformschritte an den praktischen Anforderungen hybrider Bedrohungslagen ausgerichtet werden.

Praxisgerechte Übermittlungsschwellen

Die Übermittlung personenbezogener Daten zwischen Nachrichtendiensten und Strafverfolgungsbehörden ist grundsätzlich nur zum Schutz herausragender öffentlicher Interessen und damit nur zur Verfolgung besonders schwerer Straftaten zulässig.[9] Die bestehenden Übermittlungsschwellen für BND und BfV an Staatsanwaltschaft und Polizei orientieren sich vor allem an klassischen Strafverfolgungssachverhalten und werden hybriden Bedrohungslagen nur begrenzt gerecht.

Voraussetzung für eine Übermittlung ist der auf konkreten Tatsachen beruhende Verdacht einer besonders schweren Straftat. Nach § 11a Abs. 1 BNDG und § 21 Abs. 2 BVerfSchG setzt die Übermittlung grundsätzlich Straftaten voraus, die mit einer Höchstfreiheitsstrafe von mindestens zehn Jahren bedroht sind oder – im Fall einer besonderen außen- oder sicherheitspolitischen Relevanz bzw. eines Staatsschutzbezuges – mit mindestens fünf Jahren, etwa wenn sie extremistischen oder terroristischen Zielen dienen. Für Daten aus Wohnraumüberwachungen gelten strengere Voraussetzungen.

Übermittlungshürden bei hybriden Bedrohungen

Diese Anforderungen dienen zwar dem Grundrechtsschutz, können jedoch eine frühzeitige Gefahrenerkennung erschweren. Gerade hybride Bedrohungen erfüllen die Übermittlungsvoraussetzung einer besonders schweren Straftat häufig nicht oder erst in einem fortgeschrittenen Stadium. Beispiele umfassen Delikte wie verfassungsfeindliche Sabotage, Volksverhetzung, Ausspähen von Daten, Computersabotage oder die Störung öffentlicher Betriebe.

Eine Datenübermittlung zum Zweck der Gefahrenabwehr kann dieses Defizit nur teilweise kompensieren. Zwar genügen hierfür tatsächliche Anhaltspunkte für eine zumindest konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut. Solche Übermittlungen sind jedoch nur an inländische Gefahrenabwehr- und Verwaltungsbehörden[10] zulässig (keine Strafverfolgungsbehörden) und dürfen nicht zur Umgehung der strengeren Voraussetzungen der

Datenübermittlung an Strafverfolgungsbehörden genutzt werden. Erkenntnisse über zufällig bekannt gewordene oder nicht besonders schwere Straftaten können daher nicht für Zwecke der Strafverfolgung übermittelt werden.

Die mit der letzten BNDG-Reform[11] eingeführte Übermittlungsschwelle von zehn Jahren Höchstfreiheitsstrafe war von Beginn an umstritten. Kritisiert wurde u.a. die ausschließliche Orientierung am Höchststrafrahmen. Der Auftrag der Nachrichtendienste knüpft an besonders gewichtige Gemeinwohlbelange an und lässt sich daher nur eingeschränkt anhand des Strafrahmens einzelner Delikte abbilden.

Übermittlungsschwellen praxistauglich ausgestalten

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Hessischen Verfassungsschutzgesetz[12] ausgeführt, dass eine besonders schwere Straftat regelmäßig bereits bei einer Höchstfreiheitsstrafe von mehr als fünf Jahren vorliegt. Der Referentenentwurf greift dieses Begriffsverständnis auf. Da gegenwärtig allerdings keine Straftatbestände mit einem Strafrahmen von mehr als fünf und weniger als zehn Jahren bestehen, führt diese Anpassung im Ergebnis nicht zu einer Erweiterung der Übermittlungsmöglichkeiten. Im Gegenteil: Da der Gesetzgeber zugleich die bisherigen Übermittlungsalternativen für nachrichtendienstliche Relevanz bzw. Staatsschutzbezug streicht, führt die Reform eher zu einer Einschränkung der Übermittlungsmöglichkeiten. Im weiteren Gesetzgebungsverfahren sollte daher geprüft werden, ob die vorgeschlagenen Übermittlungsschwellen den praktischen Anforderungen hybrider Bedrohungslagen hinreichend Rechnung tragen. Im Sinne praxistauglicher Übermittlungsschwellen sollte ein Begriffsverständnis fernab des Höchststrafrahmens entwickelt werden.

Von behördlicher Kooperation zu gesamtheitlicher Lagebildgenerierung

Die deutsche Sicherheitsarchitektur verfügt über zahlreiche gemeinsame Zentren, die den behördlichen Informationsaustausch und die Abstimmung in konkreten Gefährdungslagen unterstützen. Ihre Ausrichtung folgt jedoch überwiegend einzelnen Phänomenbereichen wie Terrorismus (GTAZ), Cyberabwehr (Cyber-AZ), Migration (GASIM), Bevölkerungsschutz (GeKoB/GMLZ), hybriden Bedrohungen (GAZ Hybrid) oder Drohnen (GDAZ). Die über Jahrzehnte entstandene Vielzahl spezialisierter Kooperationsstrukturen hat damit zu einer organisatorischen Zersplitterung beigetragen.

Phänomenübergreifende Zuständigkeit bei hybriden Bedrohungen

Gerade hybride Bedrohungen überschreiten regelmäßig phänomenbezogene Zuständigkeiten. Ein Drohnenüberflug kann zugleich Elemente der Spionage, Sabotage, Cyberoperationen, ausländischen Einflussnahme, allgemeiner Kriminalität oder terroristischen Motivation aufweisen und damit sowohl polizeiliche als auch nachrichtendienstliche Zuständigkeiten berühren. Das bestehende System gemeinsamer Zentren ist auf derart dynamische phänomenübergreifende Lagen nur begrenzt ausgelegt. Hinzu kommt, dass die Zusammenarbeit häufig vom persönlichen Austausch der Verbindungsbeamtinnen und -beamten abhängt, dessen personelle Abdeckung nicht jederzeit und durch jede Behörde gewährleistet werden kann. Die Verdichtung sicherheitsrelevanter Einzelinformationen zu einem gemeinsamen Risikobild bleibt dadurch vielfach ein manueller, einzelfallbezogener und ressourcenintensiver Prozess. Dies ist umso gravierender, da Bedrohungslagen zusehends informierte – und vor allem schnelle – Reaktionen erfordern.

Es bedarf daher nicht weiterer Kooperationsformate, sondern der Fähigkeit zur behörden- und phänomenübergreifenden Lagebildgenerierung. Der Referentenentwurf trägt diesem

Problem erstmals Rechnung, indem er eine gemeinsame automatisierte Auswertung zwischen BND bzw. BfV und anderen inländischen öffentlichen Stellen ermöglicht (§ 63 BNDG-E; § 42 BVerfSchG-E). Die Daten verbleiben bei der jeweils erhebenden Behörde, können jedoch für gemeinsame automatisierte Analysen genutzt werden. Damit schafft der Entwurf erstmals eine ausdrückliche Rechtsgrundlage für behördenübergreifende Analysen und verbessert die Voraussetzungen für gemeinsame Lagebilder.

Ganzheitliche Analysestelle zur systemischen Informationsverdichtung

Gleichwohl bleibt die Reform unvollständig: Weder verändert sie die organisatorisch zersplitterte Kooperationslandschaft noch schafft sie eine institutionalisierte behördenübergreifende Gesamtanalyse oder ressortübergreifende Risikobewertung. Mittelfristig sollte daher die Einrichtung einer eigenständigen Analyse- und Lagebildstelle geprüft werden. Diese könnte als organisatorisch eigenständige Struktur rechtmäßig erhobene und übermittelte Informationen aus BND, BfV, BAMAD, Bundes- und Landespolizeien, Generalbundesanwalt, Staatsanwaltschaften sowie weiteren Fachbehörden zusammenführen, analysieren und zu behördenübergreifenden Risikobewertungen verdichten. Anders als die bestehenden Kooperationszentren würde sie Informationen nicht lediglich austauschen, sondern systematisch auswerten. Zugleich bliebe das informationelle Trennungsprinzip gewahrt, da die Stelle weder selbst nachrichtendienstliche Erkenntnisse erhebt noch polizeiliche Befugnisse ausübt, sondern ausschließlich rechtmäßig übermittelte Informationen verarbeitet und die Analyseergebnisse den zuständigen Behörden zur Verfügung stellt. Auf diese Weise ließe sich die bestehende Lücke zwischen Informationsaustausch und Informationsverdichtung schließen, ohne die grundlegenden Anforderungen des Trennungsgebots aufzugeben.

5. Schlussfolgerungen für die Sicherheitsarchitektur

Die sicherheitspolitischen Rahmenbedingungen haben sich grundlegend verändert. Hybride Bedrohungen überschreiten zunehmend die traditionellen Grenzen zwischen innerer und äußerer Sicherheit und stellen eine Sicherheitsarchitektur infrage, deren Organisations- und Informationsstrukturen weitgehend entlang getrennter Zuständigkeiten ausgestaltet sind. Eine zeitgemäße Weiterentwicklung des Trennungsgebots scheint eine sicherheitspolitische Notwendigkeit zu sein.

Trennungsgebot als Rahmen, nicht als Hürde

Das informationelle Trennungsprinzip ist dabei die verfassungsrechtliche Leitplanke. Es schließt eine intensivere behördenübergreifende Zusammenarbeit jedoch nicht aus, sondern setzt den rechtlichen Rahmen für ihre Ausgestaltung. Entscheidend ist daher weniger die Ausweitung behördlicher Befugnisse als die Fähigkeit, rechtmäßig erhobene Informationen und relevante Erkenntnisse schneller zusammenzuführen, gemeinsam auszuwerten und zu belastbaren Risikobewertungen zu verdichten, um staatliches Handeln zeitnah zu ermöglichen.

Der Referentenentwurf zur Reform des Nachrichtendienstrechts enthält hierfür wichtige Ansätze. Insbesondere die erweiterten Übermittlungsmöglichkeiten und die erstmalige gesetzliche Grundlage für gemeinsame automatisierte Analysen stellen einen wesentlichen Fortschritt dar. Die organisatorische Zersplitterung der Sicherheitsarchitektur sollte stärker adressiert und ein Rahmen für eine institutionalisierte behördenübergreifende Gesamtanalyse geschaffen werden.

Eine zukunftsfähige Sicherheitsarchitektur sollte daher den nächsten Schritt gehen: standardisierte Verfahren zur frühzeitigen Erkennung hybrider Verdachtsfälle schaffen, praxistaug-

liche Übermittlungsschwellen festlegen sowie die institutionalisierte Informationsverdichtung in einer eigenständigen Analyse- und Lagebildstelle etablieren. Erst durch das Zusammenspiel dieser Elemente lässt sich die Lücke zwischen Informationsaustausch und behördenübergreifender Risikobewertung schließen, ohne die grundrechtlichen Anforderungen des Trennungsgebots aufzugeben. Mittel- und langfristig bedarf es zudem einer grundlegenden Reform der deutschen Sicherheitsarchitektur, unter Konsolidierung ihrer komplexen Organisationslandschaft und der weitgehend zersplitterten Kooperationsstrukturen. Dabei darf die bundesstaatliche Kompetenzzuordnung nicht außer Acht gelassen werden.

Konsolidierung der zersplitterten Sicherheitsarchitektur als langfristiges Ziel

1 Sowie die Verfassungsschutzbehörden der Länder.

2 Wortlaut: „The federal government will also be permitted to establish an agency to collect and disseminate information concerning subversive activities directed against the federal government. This agency shall have no police authority.".

3 Vgl. dazu u.a. Alexander Dorn: Das Trennungsgebot in verfassungshistorischer Perspektive, Berlin 2004, S. 23 sowie Christoph Gröpl: Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, Berlin 1993, S. 301-303.

4 Vgl. dazu u.a. Bernadette Droste: Handbuch des Verfassungsschutzrechts, 2007, S. 41 sowie Markus Thiel: Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 385-391.

5 Deutscher Bundestag, Wissenschaftlicher Dienst: „Sachstand: Gemeinsames Terrorismusabwehrzentrum (GTAZ) – Rechtsgrundlagen und Vergleichbarkeit mit anderen Kooperationsplattformen", WD 3 – 3000 – 406/18, 2018, S. 6.

6 In drei Landesverfassungen besitzt das Trennungsgebot dagegen Verfassungsrang: Sachsen (Art. 83 Abs. 3 VerfSN), Thüringen (Art. 97 VerfTH) und Brandenburg (Art. 11 Abs. 3 VerfBB).

7 Vgl. § 2 Abs. 1 Satz 3 BVerfSchG, § 1 Abs. 1 Satz 2 BNDG, § 1 Abs. 2 MADG für die organisatorische Dimension und § 2 Abs. 3 Satz 1 BNDG für die kompetenzielle Dimension.

8 Vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07 -, Rn. 1-233, https://www.bverfg.de/e/rs20130424_1bvr121507 (letzter Abruf: 29.07.2026).

9 Vgl. § 11a BNDG, § 21 BVerfSchG, § 33 MADG.

10 Vgl. § 11b BNDG, § 19 BVerfSchG, § 31 MADG.

11 Vgl. BGBl. I 2023, Nr. 410.

12 BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 1-245, https://www.bverfg.de/e/rs20240717_1bvr213322 (letzter Abruf 29.07.2026).

Impressum

Autorinnen und Autoren

Diese Publikation wurde von Dr. Franca König, Dr. Sandra Lukosek und Dr. Till Nierhoff aus dem Arbeitskreis „Terrorismus & Innere Sicherheit“ der Konrad-Adenauer-Stiftung e. V. verfasst.

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2026, Berlin

Kontakt:
Felix Neumann
Extremismus- und Terrorismusbekämpfung
Analyse und Beratung
Felix.Neumann@kas.de
Tel. +49 30 26996-3879

Bildnachweis Titelseite: mit der KI Adobe Firefly generiert, Konrad-Adenauer-Stiftung e. V.
Gestaltung und Satz: Konrad-Adenauer-Stiftung e. V.
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-368-1