Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)417 I

Bundespolizeipräsidium

Präsident Dr. Dieter Romann

Bundespolizeipräsidium, Heinrich-Mann-Allee 103, 14473 Potsdam

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

POSTANSCHRIFT Heinrich-Mann-Allee 103
14473 Potsdam
TEL +49 331 97 997-0
FAX +49 30 204561-1710
E-MAIL Bpolp@polizei.bund.de
INTERNET www.bundespolizei.de
ORT, DATUM Potsdam, 21. April 2024

Schriftliche Stellungnahme des
Präsidenten des Bundespolizeipräsidiums
Herrn Dr. Dieter Romann
zur öffentlichen Anhörung am 22. April 2024

zum Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetztes
BT-Drucksache 20/10406

I. Vorbemerkung

Ich begrüße sehr, dass die Bundespolizei im Zuge ihrer für unser Land bedeutenden Aufgabenwahrnehmung ein verbessertes und moderneres Befugnisinstrumentarium erhalten soll. Ich bedanke mich im Namen aller Mitarbeiterinnen und Mitarbeiter der Bundespolizei, dass in dieser Legislaturperiode der Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes aufgegriffen wurde.

Das Bundespolizeigesetz bedarf dringend der Modernisierung, da die 55.000 Beschäftigten der Bundespolizei gegenwärtig bei der Wahrnehmung hoheitlicher Aufgaben – insofern der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung in ihrem Zuständigkeitsbereich – ein Bundespolizeigesetz anwenden, welches zum überwiegenden Teil noch aus dem Jahr 1994 stammt.

II. Zum Inhalt des Gesetzentwurfs

Der Gesetzentwurf enthält zahlreiche neue Befugnisse die für die Bundespolizei zur Wahrnehmung hoheitlicher Aufgaben von herausragender Bedeutung sind. Insbesondere ist sehr zu begrüßen, dass umfassende neue Datenverarbeitungsregeln, nach verfassungsrechtlichen Vorgaben (§ 42 ff. BPolG-E), insbesondere unter Beachtung des “Grundsatzes der hypothetischen Datenneuerhebung“, gemäß Urteil des BVerfG vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09) aufgenommen wurden. Insbesondere sind die Verbesserung der Liegenschaftssituation (§ 96 BPolG-E), die Ingewahrsamnahme auch zur Durchsetzung eines Aufenthaltsverbotes oder einer Meldeauflage (§ 60 BPolG-E), die Erweiterung der Anlasstaten für den verlängerten Unterbindungsgewahrsam (§ 64 BPolG-E) sowie die Temporären Meldeauflagen (§ 29 BPolG-E) und Aufenthaltsverbote (§ 59 BPolG-E) zu nennen. Mit der präventiven Telekommunikationsüberwachung (§ 40 BPolG-E) wurde bereits ein kleiner erster Grundstein für noch fehlende „Cyberbefugnisse“ gelegt.

III. Prioritäre Ergänzungsvorschläge

1. Cyberabwehrbefugnisse

Cyberangriffe nehmen insbesondere in der derzeitigen (geo-) politischen Lage zu. Angriffen auf die Sicherheit der Informationstechnik in Deutschland muss mit entsprechenden technischen aber auch rechtlichen Instrumentarien entgegengetreten werden. Angesichts der aktuellen Bedrohungslage bedarf es umso mehr zügigem Handeln, um den rechtlichen Befugnisrahmen der Bundespolizei anzupassen. Innerhalb des bestehenden Aufgabenbereichs der Bundespolizei bedarf es neuer Befugnisse für die Abwehr von schwerwiegenden Gefahren für die Sicherheit in der Informationstechnik.

Zielführend erscheint es jedoch, diese Anpassungen jetzt schon in den bestehenden Gesetzentwurf aufzunehmen; die Bedrohungslage wartet nicht auf eine für andere Bundessicherheitsbehörden erforderliche Verfassungsänderung zur Gefahrenabwehr und auf fehlende einfachgesetzliche Anpassungen der rechtlichen Befugnisnormen für die Bundespolizei.

Die Bundespolizei braucht Cyberabwehrbefugnisse in ihrem Aufgabenbereich, damit sie in die Lage versetzt wird, jetzt schon in der digitalen Befugniswelt genauso handlungsfähig zu sein, wie spiegelbildlich im Analogen.

Daher sollten diese angestrebten Änderungen für das BPolG in diesen Entwurf aufgenommen werden, um nicht noch mehr Zeit im Kampf gegen die hybride Verbrechenswelt zu verlieren.

Für die Befugniserweiterung im Aufgabenbereich der Bundespolizei ist keine GG-Änderung erforderlich, da hier ihre gefahrenabwehrrechtliche Zuständigkeit der Bundespolizei unverändert bleibt und lediglich in digitale Befugnisse transferiert werden muss. Die Gelegenheit sollte daher hier und jetzt ergriffen werden. Die Modernisierung des BPolG bietet sich an, um diese einfachgesetzliche Änderung zu normieren, die in der letzten Legislaturperiode bereits abgestimmt war.

Konkrete Formulierungsvorschläge samt Begründung zu §§ 41a ff. BPolG-E nachfolgend unter Ziffer IV.

2. Befugnis zur Beantragung von Haft zur vorübergehenden Sicherung der Abschiebung bei Inlandsaufgriffen

Das Gesetz zur Verbesserung der Rückführung mit entsprechenden Änderungen im Aufenthaltsgesetz trat jüngst in Kraft.

Ziel des Gesetzes ist, Abschiebungen zu vereinfachen, es sieht z. B. eine einfachere Ausweisung von Straftätern, Rückführungen ohne vorherige Ankündigungen, erweiterte Durchsuchungsmöglichkeiten vor und erweitert Haftgründe.

Generell besteht Einigkeit, dass insbesondere Straftäter, die vollziehbar ausreisepflichtig sind, zeitnah zurückgeführt werden müssen, dass Schleusungskriminalität mit aller Härte begegnet werden muss.

Durch die bereits 2021 vorgeschlagene Erweiterung der Abschiebehaft kann die Bundespolizei in diesem Gefüge einen sinnvollen gesamtstaatlichen Beitrag zu diesem gesetzlich verfolgten Ziel leisten.

In Deutschland halten sich mit Stand 31. März 2024 insgesamt 233.712 vollziehbar ausreisepflichtige Drittstaatsangehörige auf; dabei 45.892 ohne Duldung.

Eben diese Personen werden im Rahmen der Aufgabenerfüllung der Bundespolizei täglich im Inland aufgegriffen. Vornehmlich im Bahnhofsmilieu, insbesondere zur Nachtzeit und an Wochenenden in Großstädten. Sofern dies jedoch außerhalb der üblichen Geschäftszeiten der zuständigen Ausländerbehörden erfolgt, kann die insoweit befugnislose Bundespolizei lediglich eine sog. Anlaufbescheinigung ausstellen. Im Ergebnis können sich diese Personen dann dem behördlichen Prozess leicht entziehen und bleiben am Abschiebetag unauffindbar.

Um die Zielrichtung des Rückführungsverbesserungsgesetzes nicht zu unterlaufen, ist es daher geboten, der Bundespolizei eine temporäre Befugnis (d.h. bei Gefahr in Verzug) zur Beantragung von Haft zur Sicherung der Abschiebung einzuräumen.

Es geht hierbei nicht um die Übertragung einer neuen Aufgabe. Die Ausländerbehörden bleiben selbstverständlich weiter zuständig. Die Bundespolizei erlangt dadurch auch keine Zuständigkeit zur Strafverfolgung des unerlaubten Aufenthalts. Es geht dabei nur um ein Einfrieren – „QUICK FREEZE“ – der Situation, damit ein unerlaubt aufhältiger vollziehbar ausreisepflichtiger Drittstaatsangehöriger ohne Duldung solange mit richterlichen Beschluss sistiert wird, bis die zuständige Landesbehörde wieder erreichbar ist. Am Negativbeispiel Anis AMRI wurde der ganzen Welt in dramatischer Form aufgeführt, welche Konsequenzen das haben kann. Die Bundespolizei kann auch gegenüber dem Gericht Angaben dazu machen, in welchem Zeitraum die Beschaffung von Passersatzpapieren erfolgen kann.

Konkrete Formulierungsvorschläge samt Begründung zu § 71 Abs. 3a AufenthG-E nachfolgend unter Ziffer IV.

3. Gekorene Zuständigkeit

Der für die Bundespolizei zusätzlich wichtige Ergänzungspunkt ist die Regelung zur Übernahme der Strafverfolgung in Einzelsachverhalten auf Ersuchen der zuständigen Staatsanwaltschaft, die hier als gekorene Zuständigkeit bezeichnet wird.

Mit dieser faktischen und kompetenzrechtlich unbedenklichen Amtshilfe in Einzelfällen werden die Länder nur auf deren eigenen staatsanwaltschaftlichen Antrag entlastet und bleiben verfahrensleitend. Insbesondere können länderübergreifende komplexe strafrechtsrelevante Sachverhalte unter der Sachleitung der federführenden Staatsanwaltschaft bei einer Ermittlungsbehörde zusammengeführt werden. Beispielhaft aus der Praxis sind grenz- und länderübergreifende Tätergruppierungen, die sich auf Fahrkartenautomatenaufbrüche und -sprengungen, aber auch auf Geldautomatenaufbrüche und -sprengungen in Bahnhofsnähe konzentriert haben. Hierbei kommt zusätzlich die grenz- und bahnpolizeiliche Expertise auch in der Strafverfolgung zum Tragen. Gleiches kann gelten für Straftaten wie Schleusungskriminalität in Verbindung mit Urkunden oder sonstiger milieubedingter Kriminalität (u.a. Clanbereiche). Bei Drittstaatsangehörigen können zudem nach der Strafvollstreckung Synergieeffekte im Bereich der Rückführung erzielt werden.

Konkrete Formulierungsvorschläge samt Begründung zu § 13 BPolG-E nachfolgend unter Ziffer IV.

4. Sicherheitsforschung in der Bundespolizei

Bestimmte bundespolizeiliche Aufgaben erfordern die Gewinnung wissenschaftlicher Erkenntnisse mit direktem Bezug zu eigenen Tätigkeitsfeldern und sind Voraussetzung zur Erfüllung eigener Fachaufgaben. Die Beschränkung alleinig auf die Thematik Luftsicherheit greift inhaltlich und sachlich zu kurz. Wesentliche Interessens- und gesetzliche Aufgabengebiete der Bundespolizei, die auch nicht durch andere Behörden abgedeckt werden, blieben außen vor.

Im Gesetzesentwurf von 2020 war jedoch die Legitimation für die Forschung der Bundespolizei für den gesamten Aufgabenbereich abgedeckt. Diese Formulierung ist gegenüber der nunmehr dargestellten Formulierung deutlich zu bevorzugen und wäre abschließend.

Eine zentrale Einrichtung ist mit der Forschungs- und Erprobungsstelle der Bundespolizei in Lübeck bereits etabliert. Die vorgesehene gesetzliche Grundlage beschränkt sich allein und nur auf die Luftsicherheit. Unser Forschungsbedarf geht aber viel weiter für allen Aufgaben der Bundespolizei. Darunter auch Aufgabengebiete, die von anderen Behörden nicht abgedeckt werden, z. B. Schutz maritimer Infrastrukturen auf See, Schutzausrüstung für die

CBRN-Entschärfter GSG 9 oder Unterwasseraufklärungstechnologie oder im Bereich nonletaler Wirkmittel.

Konkrete Formulierungsvorschläge samt Begründung zu § 1 Abs. 9 BPolG-E nachfolgend unter Ziffer IV.

IV. Konkrete Formulierungsvorschläge

1. Cyberabwehrbefugnisse

Es wird empfohlen nach § 41 BPOLG-E folgende Paragraphen schon in den bestehenden Gesetzentwurf aufzunehmen:

§ 41a

Mitwirkung Verpflichteter bei der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik

(1) Die Bundespolizei kann zur Erfüllung ihrer Aufgaben nach § 1 Absätze 3 bis 6 sowie den §§ 2 bis 8, wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt oder für die Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Anzahl von Personen erforderlich ist, die nach § 170 Absatz 9 Telekommunikationsgesetz zur Mitwirkung verpflichteten Stellen anweisen, den Datenstrom über deren Netze oder informationstechnischen Systemen, die für die Verwirklichung von Straftaten nach den §§ 202a, 202b, 202c, 202d, 263a, 303a und 303b des Strafgesetzbuchs genutzt werden und die sich richten gegen

1. *die innere und äußere Sicherheit der Bundesrepublik Deutschland,*
2. *sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen oder Behörden des Bundes, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist, oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, oder*
3. *die Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Anzahl von Personen,*

auf eine von der Bundespolizei vorgegebene Zieladresse umzuleiten, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. Die Bundespoli-

zei setzt sich bei der Anordnung der Maßnahme mit dem Bundesamt für Sicherheit in der Informationstechnik ins Benehmen. Unter den Voraussetzungen der Sätze 1 bis 3 kann die Bundespolizei nach Maßgabe des § 20 die Maßnahme auch selbst vornehmen.

(2) Die Maßnahme nach Absatz 1 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 23 Absatz 2 und des § 37 Absatz 2 entsprechend. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung durch die nach Satz 1 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit diese Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(3) Die Bundespolizei darf Daten, die nach Absatz 1 umgeleitet wurden, verarbeiten, um Informationen über betroffene informationstechnische Systeme, Schadprogramme oder Angriffswege zu erlangen oder um von einer Maßnahme Betroffene oder durch eine Straftat nach Absatz 1 Geschädigte zu informieren. Sie darf diese Daten an andere Behörden, die mit der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik befasst sind, übermitteln, sofern dies für deren Aufgabenerfüllung erforderlich ist.

(4) Eine über die im vorstehenden Absatz hinausgehende Verarbeitung zu anderen Zwecken ist unbeschadet der Vorschriften in Abschnitt 2 Titel 2 unzulässig. Soweit möglich ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahme nach Absatz 1 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist. Die Bundespolizei unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.

(5) Die Bundespolizei darf Daten, die nach Absatz 1 umgeleitet wurden, an das Bundesamt für Sicherheit in der Informationstechnik übermitteln, sofern dies für die Aufgabenerfüllung des Bundesamts für Sicherheit in der Informationstechnik erforderlich ist.

(6) Die Verpflichteten nach Absatz 1 haben, soweit dies erforderlich ist, über die Verpflichtung nach § 24 und § 25 hinaus auf Ersuchen der Bundespolizei an den Maßnahmen nach §§ 41a Absatz 1, 41b Absatz 1 sowie 41c Absatz 1 mitzuwirken. § 40 Absatz 5 gilt entsprechend.

Nicht nach dem Telekommunikationsgesetz Verpflichtete dürfen nur nach den zusätzlichen Voraussetzungen des § 21 in Anspruch genommen werden.

§ 41b

Eingriffe in informationstechnische Systeme

(1) Die Bundespolizei kann ohne Wissen des Betroffenen mit technischen Mitteln in informationstechnische Systeme eingreifen und dort Daten erheben, speichern, löschen oder verändern, wenn Tatsachen die Annahme rechtfertigen, dass sie zur Verwirklichung einer Straftat nach § 41a Absatz 1 verwendet werden sollen und von ihnen eine dringende Gefahr für

1. *den Bestand oder die Sicherheit des Bundes oder eines Landes,*
2. *Leib, Leben oder Freiheit einer Person,*
3. *Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt oder für die Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Anzahl von Personen,*
4. *solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt oder*

ausgeht.

Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung der Bundespolizei erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre. § 41a Absatz 1 Satz 2 bis 4 gelten entsprechend.

(2) Die Maßnahmen nach Absatz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 23 Absatz 2 und des § 37 Absatz 2 entsprechend. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung durch die nach Satz 1 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit diese Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(3) Die Bundespolizei darf Daten, die nach Absatz 1 erlangt wurden, verarbeiten, um Informationen über betroffene informationstechnische Systeme, Schadprogramme oder Angriffswege zu erlangen oder von einer Maßnahme Betroffene oder durch eine Straftat nach § 41 a Absatz 1 Geschädigte zu informieren.

(4) Es ist technisch sicherzustellen, dass

1. *an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Erhebung, Löschung und Veränderung der Daten unerlässlich sind, und*

2. *die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.*

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. § 41a Absatz 3 Sätze 2 bis 6 gelten entsprechend.

§ 41c

Einschränkung von IT-Systemen bei Gefahren für die Sicherheit in der Informationstechnik

(1) Die Bundespolizei kann zur Erfüllung ihrer Aufgaben nach § 1 Absätzen 3 bis 6 sowie den §§ 2 bis 8 den Betrieb eines informationstechnischen Systems ohne Wissen des Betroffenen einschränken, untersagen oder unterbinden, wenn Tatsachen die Annahme rechtfertigen, dass von dem informationstechnischen System eine dringende Gefahr ausgeht. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 41a Absatz 1 erforderlich ist. Sie ist nach Wegfall der Gefahr unverzüglich aufzuheben. § 41a Absatz 1 Satz 2 bis 4 gelten entsprechend.

(2) Die Maßnahmen nach Absatz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 23 Absatz 2 und des § 37 Absatz 2 entsprechend. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung durch die nach Satz 1 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit diese Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(3) Im Antrag nach Absatz 2 sind anzugeben:

1. *die Kennung des Anschlusses oder des informationstechnischen Systems, von dem eine Gefahr ausgeht oder auf das der Angriff auf die Sicherheit in der Informationstechnik gerichtet ist,*

2. *Art, Umfang und Dauer der Maßnahme,*

3. *der Sachverhalt sowie*

4. *eine Begründung.*

(4) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. *die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, von dem eine Gefahr ausgeht oder auf das der Angriff auf die Sicherheit in der Informationstechnik gerichtet ist,*

2. *Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,*

3. *der Sachverhalt sowie*

4. *die wesentlichen Gründe.“*

1. *§ 77 Absatz 1 wird wie folgt geändert:*

   a) *Die Angabe „41“ wird gelöscht.*

   b) *Nach der Angabe „40“ wird ein „bis 41c“ eingefügt.*

   c) *Nach Nummer 6 wird folgende Nummer 7 neu eingefügt:*

   „7. des § 41a (Mitwirkung Verpflichteter bei der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik), § 41b (Eingriffe in informationstechnische Systeme, § 41c (Einschränkung von IT-Systemen bei Gefahren für die Sicherheit in der Informationstechnik)

   a) der Nutzer und der Inhaber des informationstechnischen Systems, von dem die Gefahr ausgeht,

   b) der Inhaber des informationstechnischen Systems, auf das der Angriff gerichtet ist

   c) der Nutzer und der Inhaber des informationstechnischen Systems, dessen Betrieb eingeschränkt oder unterbunden wurde“.

   d) *Die vorhergehende Nummer „7“ wird zu Nummer „8“.*

2. *§ 80 wird wie folgt geändert:*

a) In Absatz 1 Satz 1 wird nach der Angabe „41“ ein „c“ eingefügt.

b) In Absatz 2 Ziffer 2 wird nach der Angabe „41“ ein „c“ eingefügt.

3. § 84 wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „41“ gelöscht.

b) In Absatz 1 Satz 1 wird nach der Angabe „40“ ein „bis 41c“ eingefügt.

c) Nach Absatz 2 Ziffer 6 wird folgende Nummer 7 eingefügt:

„7. bei Maßnahmen nach den §§ 41a (Mitwirkung Verpflichteter bei der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik), 41b (Eingriffe in informationstechnische Systeme, 41c (Einschränkung von IT-Systemen bei Gefahren für die Sicherheit in der Informationstechnik)

a) der Nutzer und der Inhaber des informationstechnischen Systems, von dem die Gefahr ausgeht,

b) der Inhaber des informationstechnischen Systems, auf das der Angriff gerichtet ist

c) der Nutzer und der Inhaber des informationstechnischen Systems, dessen Betrieb eingeschränkt oder unterbunden wurde“.

c) Die vorhergehende Nummer „7“ wird zu Nummer „8“.

4. § 104 Absatz 1 wird wie folgt geändert:

a) Nach Nummer 2 werden folgende Nummern ergänzt:

„3. einer vollziehbaren Anordnung nach § 41a Absatz 1 und § 41c Absatz 1 zuwiderhandelt,

4. wer entgegen § 41c Absatz 1 ein IT-System betreibt, das zur Begehung einer Straftat nach § 41a Absatz 1 verwendet wird und von dem eine dringende Gefahr ausgeht, entgegen einer vollziehbaren Anordnung betreibt.“

b) Nach Absatz 2 wird folgender Absatz ergänzt:

„(2a) Verstöße gegen die Bestimmungen des Absatzes 1 Nummer 4 kann mit Geldbußen von bis zu 20 000 000 EURO geahndet werden. Verstöße gegen die Bestimmungen des Absatzes 1 Nummer 3 können mit Geldbußen von bis zu 10 000 000 EURO geahndet werden.“

5. In § 106 wird in Absatz 1 Satz 1 nach der Angabe „41“ ein „c“ eingefügt.

Begründung:

Mit den neu hinzuzufügenden § 41a, § 41b und § 41c erhält die Bundespolizei Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik im Rahmen ihrer bestehenden Aufgaben nach den § 1 Abs. 3 bis 6 sowie den §§ 2 bis 8 BPolG-neu. Diese Anpassung trägt der zunehmenden Anzahl von Bedrohungen aus dem Cyberraum Rechnung, auf die die Bundespolizei im Rahmen ihrer bestehenden Zuständigkeiten mit adäquaten Befugnissen reagieren können muss. Die Gefahrenabwehrzuständigkeiten der Länder werden durch die Befugnisergänzung nicht berührt, Feststellungen im Zuständigkeitsbereich der Länder werden, wie bei analogen Sachverhalten, an die jeweils zuständige Stelle abgegeben.

Bereits heute ist die Bundespolizei darauf angewiesen, Gefahren aus dem Cyberraum – die ihre Aufgabenwahrnehmung beeinträchtigen könnten – durch vorsorgende Maßnahmen zu begegnen. Nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik ist die Bundespolizei etwa gehalten, die Integrität, die Verfügbarkeit und die Vertraulichkeit ihrer Informationen zu schützen, um somit die Funktionsfähigkeit der Bundespolizei und eine effektive Aufgabenerfüllung sicherstellen zu können. Darüber hinaus setzt die Bundespolizei Cyber-Fähigkeiten zur Strafverfolgung, zur Sicherung eigener Einrichtungen und zur Unterstützung anderer Behörden erfolgreich ein.

Infolge der fortschreitenden technologischen Entwicklung bestehen vielfältige Einwirkungsmöglichkeiten aus dem Cyberraum, die sämtliche Aufgabenbereiche der Bundespolizei betreffen. Hieraus ergibt sich die Notwendigkeit weitergehender Befugnisse. Beispielsweise besteht im Rahmen der Aufgabenwahrnehmung nach § 2 BPolG die Notwendigkeit zur Abwehr von Gefahren für biometriegestützte Grenzkontrollsysteme oder sonstige Einrichtungen der Grenzkontrolle. Denkbar sind ferner im Rahmen der Aufgabenwahrnehmung Angriffe auf informationstechnische Systeme der Bahn oder des Luft- und Seeverkehrs. Die Schaffung der hierzu notwendigen Befugnisnormen ist daher unabdingbar.

Sachverhalte, die Maßnahmen nach dieser Vorschrift erfordern, sind in der Regel andauernde, komplexe Angriffe auf die Sicherheit in der Informationstechnik. In vielen Fällen werden die konkreten Störungen noch nicht erkennbar sein. Akteure, die zu solchen Angriffen fähig sind, sind dauerhaft aktiv, entwickeln die Angriffsinfrastrukturen permanent weiter und bedienen sich hierbei verschiedener Verschlüsselungsverfahren. Charakteristisch für diese andauernden, komplexen Bedrohungskampagnen ist aus technischer Sicht, dass Schadsoftware in Opfersysteme eingebracht wird, welche sich über einen oder mehrere Proxyserver (Weiterleitungsserver) verbindet und direkt über das Internet erreichbar ist. Die Datenkommunikation ist in der Regel bereits verschlüsselt. Der Letzte in einer Kette von Proxy-Servern verbindet sich oftmals über ein weiteres Verschlüsselungsverfahren (VPN-Zugangstechnik) mit einem VPN-Server (Virtual Private Network), welcher das Tor in ein ver-

schlüsseltes Netzwerk öffnet. Diese Netzwerke enthalten regelmäßig den oder verschiedenen Steuerungsserver (Command & Control Server), welcher Befehle für weitere Aktionen auf den von den Angriffen bedrohten IT-Systemen entgegennimmt bzw. den Angreifern Informationen aus diesen Systemen bereitstellt. Ein Angreifer meldet sich typischerweise über eine ähnliche Infrastrukturkette in dieses Netzwerk an. Über den dargestellten Aufbau kann der für Maßnahmen zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik relevante Steuerungsserver nicht mehr direkt im Internet angesprochen bzw. aufgeklärt (detektiert) werden. Der Betrieb solcher Server erfolgt weitgehend anonym.

Um die hieraus möglichen Gefahrenlagen wirksam abzuwehren, ist es erforderlich, Schwachstellen in der Software der Angreiferinfrastrukturen zu suchen, die Infrastruktur (Angreifer-IT zu bedrohten IT-Systemen) möglichst umfassend aufzuklären bzw. ein Monitoring bedrohter IT-Systeme zu ermöglichen bzw. sofern technisch umsetzbar, auch unmittelbaren Zugriff auf die Inhalte des Servers bzw. das Angreifernetzwerk zu erhalten. Der Angriff, welcher durch mehrere verschiedene IT-Systeme organisiert ist, kann im Idealfall nach entsprechender Aufklärung an verschiedenen Stellen unterbrochen werden. Die Identifizierung entsprechender IT-Systeme ist regelmäßig eindeutig möglich (IP-Adressen, Adressbereiche, spezifische Netzwerkmerkmale, Schadsoftwaresignaturen wie beispielsweise Hashwerte, Cookies, verwendete User-Agents, etc.). Das heißt, anhand individueller Signaturen (mit möglichem Personenbezug) können Metadaten des Telekommunikations- oder Netzwerkverkehrs gefiltert werden, um bedrohte IT-Systeme eindeutig zu identifizieren.

Bis zum Eintritt einer konkreten IT-Störung, die bei ungehindertem Verlauf geeignet wäre, erhebliche Rechtsgüterverletzungen hervorzurufen, durchlaufen Angriffe auf die Sicherheit in der Informationstechnik üblicherweise mehrere Phasen. Um die Störung abwehren zu können, sind (ohne dass bereits die konkrete Störung eingetreten ist) IT-forensische Analysen notwendig und bei Vorliegen der rechtlichen Voraussetzungen auch Zugriffe auf verschlüsselte Kommunikation zwingend erforderlich. Sofortige „Abschaltmaßnahmen“ sind technisch oftmals nicht möglich, oder aufgrund der noch unzureichenden Aufklärung gegen die Systeme der Angreifer hinsichtlich der technischen Folgen noch nicht abschätzbar. Auf welchem konkreten Weg eine IT-Bedrohung oder IT-Störung abgewendet werden kann, hängt vom Einzelfall ab (Aufklärungsergebnisse, Zugangsmöglichkeiten zu informationstechnischen-Systemen und Netzen). Darüber hinaus ist denkbar, dass Angreifer die Zugriffe durch die Polizei ihrerseits detektieren und auf andere Systeme oder Server-Ketten ausweichen.

Betroffene Personen im Sinne dieser Vorschrift sind die Betreiber der informationstechnischen Systeme, gegen welche die Maßnahmen dieser Vorschrift angewandt werden können. Dies können sowohl die informationstechnischen Systeme sein, von denen Gefahren für die Sicherheit in der Informationstechnik ausgehen, als auch die von Gefahren für die Sicherheit in der Informationstechnik betroffene informationstechnische Systeme selbst.

Zu § 41a (Mitwirkung Verpflichteter bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik)

Zu Absatz 1

Die Norm gibt der Bundespolizei die Möglichkeit durch Anordnungen gegenüber den verpflichteten Telekommunikationsdiensteanbietern bei Gefahren für die Sicherheit in der Informationstechnik in ihrem originären Aufgabenbereich den Transportweg von Datenverkehr, der eine Gefahr für die Sicherheit in der Informationstechnik verursacht, zu verändern. Ziel der Maßnahme ist entweder die Umleitung des Datenverkehrs zwischen informationstechnischen Systemen mit dem Zweck des Verwerfens oder die Umleitung des Datenverkehrs auf ein anderes Zielsystem zur Auswertung bzw. Analyse der transportieren Daten.

So kann etwa im Zusammenhang mit Maßnahmen zur Bereinigung von mit Malware infizierten Computersystemen (Botnetz) nach Sicherstellung der im Kontext des Steuerungssystems des Botnetzes (Command & Control-Server, C&C-Server) genutzten Domain der maliziöse Datenverkehr auf ein polizeilich kontrolliertes System bzw. an ein sog. Sinkhole umgeleitet werden.

Grundsätzlich sieht Satz 1 die Durchführung unter Mitwirkung der nach § 170 Absatz 1 und 2 TKG Verpflichteten vor. Hierdurch wird gewährleistet, dass die Bundespolizei insbesondere in Fällen, in denen eine Anweisung an eine andere Stelle eine bessere und/ oder schnellere Lösung zur Gefahrenabwehr bietet, auch Dritte zur Mitwirkung verpflichten kann.

Telekommunikationsdiensteanbieter, die nicht nach § 170 Absatz 1 und 2 TKG zur Mitwirkung verpflichtet sind und Telemediendiensteanbieter können unter den Voraussetzungen des § 21 BPolG-neu in Anspruch genommen werden. In bestimmten Fällen kann nach Satz 4 dennoch eine Selbstvornahme durch die Bundespolizei erforderlich sein. Hierunter fallen z.B. Konstellationen, in denen Telekommunikationsdiensteanbieter nach § 170 Absatz 1 und 2 TKG nicht verpflichtet werden können oder die Selbstvornahme durch die Bundespolizei im Rahmen der Verhältnismäßigkeit ein milderes Mittel darstellt.

Im Einzelfall können Störungen oder unmittelbar bevorstehende Gefahren für die Sicherheit in der Informationstechnik auf die durch die Bundespolizei zu schützenden Infrastrukturen bereits abgewendet werden, wenn Datenverkehre technisch (u.a. mittels Änderung von Routen oder DNS-Einträgen) umgeleitet werden.

Mit Zurückverfolgen ist die Feststellung des Ursprungs des Angriffs auf die Sicherheit in der Informationstechnik gemeint. Neben Sensorsystemen müssen hierzu gegebenenfalls die Kommunikationsverbindungen der Angreifer zu IT-Systemen im Angriffskontext sowie die Kommunikationsver-

bindungen der IT-Systeme im Angriffskontext zu den vom Angriff auf die Sicherheit in der Informationstechnik bedrohten IT-Systemen aufgezeichnet werden können, um Rückschlüsse auf den Angreifer oder auf typische Angriffsmuster ziehen zu können. Die Maßnahme zielt dabei auch auf die Erhebung, Speicherung und Auswertung des Datenverkehrs zwischen Angreifer und bedrohtem IT-System ab.

Gegebenenfalls können IT-Systeme unbeteiligter Dritter betroffen sein, wenn bspw. der Datenverkehr über diese abgewickelt wird. Durch Absatz 1 Satz 6 wird auch in diesen Fällen die Abwehr von Gefahren für die Sicherheit in der Informationstechnik ermöglicht. Im Gegensatz zu den hinter den § 41b Absatz 1 und § 41c Absatz 1 stehenden Sachverhalten geht in den Fällen des Absatzes 1 Satz 6 die Gefahr nicht von dem informationstechnischen System ursprünglich aus, gegen das die Maßnahmen gerichtet sind. Die durch Absatz 1 Satz 6 einbezogenen informationstechnischen Systeme sind somit nicht unmittelbare Tatmittel zur Begehung eines Angriffs auf die Sicherheit in der Informationstechnik. Den Sachverhalten des Absatzes 1 Satz 6 liegt somit im Gegensatz zu den Sachverhalten der § 41 b Absatz 1 und § 41c Absatz 1 eine mit der Rechtsprechung des Bundesverfassungsgerichts zur Online-Durchsuchung vergleichbare Interessenslage zugrunde, so dass etwaige Maßnahmen nur unter den dort aufgestellten Grundsätzen möglich sind.

Nach Satz 2 darf die Maßnahme nach Satz 1 auch dann durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. Denn informationstechnische Systeme, gegen die sich Maßnahmen nach Satz 1 richten, sind nicht zwangsläufig die Systeme, von denen ursprünglich die Gefahr ausging. So können IT-Systeme unbeteiligter Dritter betroffen sein, wenn der Datenverkehr über diese geroutet wird.

Nach Satz 3 setzt sich die Bundespolizei bei Anordnung der Maßnahme mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ins Benehmen. Dadurch wird sichergestellt, dass das BSI über die Durchführung der Maßnahme durch die Bundespolizei unterrichtet wird.

Zu Absatz 2

Nach Absatz 2 ergeht die gerichtliche Anordnung über die Maßnahme nach 41a Absatz 1 auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung. Bei Gefahr im Verzug kann die Anordnung durch ebendiese selbst getroffen werden, wobei eine gerichtliche Entscheidung binnen drei Tagen nachzuholen ist.

Zu Absatz 3

Die Vorschrift regelt die Befugnis zur Weiterverarbeitung der nach Absatz 1 umgeleiteten Daten. Diese werden ausgewertet um Informationen über betroffene informationstechnische Systeme zur Identifizierung, Bereinigung sowie genutzter Schadprogramme oder IT-Angriffsmustern und -werkzeugen zu erlangen.

Bei den zu analysierenden Daten handelt es sich in der Regel um Steuerungsinformationen der Schadprogramme, mit denen die betroffenen informationstechnischen Systeme infiziert sind. Umfasst sind regelmäßig auch IP-Adressen oder andere Internetkennungen der informationstechnischen Systeme, die zu einem Botnetz zusammengeschlossen sind. Je nach Schadprogramm ist es nicht ausgeschlossen, dass auch andere auf den betroffenen Systemen gespeicherte Informationen in den umgeleiteten Daten enthalten sind. Es ist beispielsweise vorstellbar, dass Schadsoftware Zugangsdaten von den infizierten Systemen (Bots) an die C&C-Server leitet.

Wird Datenverkehr auf eine von der Bundespolizei vorgegebene Zieladresse umgeleitet, kann die Datenverarbeitung auch mit dem Ziel erfolgen, den von der Maßnahme nach Absatz 1 Betroffenen zu benachrichtigen sowie die Geschädigten darüber zu informieren, dass sie Opfer einer Straftat im Sinne von Absatz 1 wurden. Die Informationsweitergabe dient ferner dem Ziel, die zumeist neben der Schadsoftware zur Übernahme des Opfersystems nachgeladene Schadsoftware zu entfernen.

Zu Absatz 4

Obgleich nach polizeilicher Erfahrung mit Blick auf die Daten, die nach Absatz 1 zur Bundespolizei umgeleitet werden, der Kernbereich privater Lebensgestaltung in aller Regel nicht berührt wird, sieht Absatz 4 eine Kernbereichsschutzregelung vor. So wird sichergestellt, dass den Vorgaben des Bundesverfassungsgerichts in seinem Urteil zum BKAG vom 20. April 2016 – 1 BvR 966/09 u. a. – (BVerfG, NJW 2016, 1781 ff.) Genüge geleitet und einer wirksamen Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gewährleistet wird.

Zu Absatz 5

Absatz 5 regelt zudem die Befugnis der Bundespolizei zur Übermittlung von nach Absatz 1 umgeleiteten Daten an das BSI. Diese erfolgt zum Zweck der Information Geschädigter. In diesen Fällen obliegt es dem BSI im Rahmen seiner Aufgabe nach § 3 Absatz 1 Nr. 14 BSIG, u.a. die für die übermittelten IP-Adressen zuständigen Provider bzw. CERTs zu benachrichtigen und aufzufordern, die gesetzlich vorgesehene Benachrichtigung der betroffenen Kunden vorzunehmen.

Zu Absatz 6

Absatz 6 Satz 1 regelt die Mitwirkungsverpflichtung von Telekommunikationsdiensteanbietern an Maßnahmen nach den §§ 41a Absatz 1, 41b Absatz 1 und 41c Absatz 1 über die Verpflichtung nach den §§ 24 und 25 BPolG-neu hinaus.

Satz 3 verweist auf § 41 Absatz 5 BPolG-neu. Entsprechend hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, der Bundespolizei die Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-

Überwachungsverordnung. Für die Entschädigung der Telekommunikationsdiensteanbieter ist § 23 des Justizvergütungs- und Entschädigungsgesetzes entsprechend anzuwenden.

Nach Satz 4 dürfen nicht nach dem TKG Verpflichtete und Telemediendiensteanbieter nur nach den zusätzlichen Voraussetzungen der in § 21 BPolG-neu geregelten Inanspruchnahme nicht verantwortlicher Personen in Anspruch genommen werden, d.h. wenn eine dringende Gefahr abzuwehren ist, Maßnahmen gegen den Verpflichteten nach TKG nicht oder nicht rechtzeitig möglich sind oder keinen Erfolg versprechen, die Bundespolizei die Gefahr nicht oder nicht rechtzeitig selbst oder durch einen Beauftragten abwehren kann und die Betroffenen ohne erhebliche eigene Gefährdung und ohne Verletzung höherwertiger Pflichten in Anspruch genommen werden können.

Zu § 41b (Eingriffe in informationstechnische Systeme)

Zu Absatz 1

Nach Absatz 1 wird der Bundespolizei die Befugnis eingeräumt, mit technischen Mitteln in informationstechnische Systeme einzugreifen, um Daten zu erheben, zu verändern oder zu löschen, sofern eine Gefahr für die Sicherheit in der Informationstechnik nicht durch mildere Mittel abgewehrt werden kann. Diese Maßnahme zielt sowohl auf informationstechnische Systeme von Angreifern wie auch diejenigen von Geschädigten.

Ein Eingreifen bedeutet das Eindringen oder Aufschalten auf ein informationstechnisches System vorzunehmen, in der Regel durch Überwindung einer Zugangsbarriere, wie zum Beispiel einem Passwort. Der Absatz 2 ermöglicht weiter aus informationstechnischen Systemen Daten zu erheben, zu übernehmen, zu löschen und zu verändern. Entsprechende Befugnisse sind z.B. in Fällen erforderlich, in denen ein informationstechnisches System mit einem Schadprogramm infiziert ist, dessen Löschung einen Angriff auf die Sicherheit in der Informationstechnik verhindern oder beenden würde.

Ein Eingreifen zur Speicherung von Daten wie IP-Adressen, Benutzernamen, Passwörtern oder Konfigurationsdaten kann im Einzelfall geeignet und erforderlich sein, um beispielsweise die Command & Control-Software in ihrer Funktionsweise zu analysieren und um Schwachstellen in der Infrastruktur des Angreifers zu suchen.

Ein Eingreifen zur Veränderung oder zum Löschen von Daten erfordert im Einzelfall tatsächliche Anhaltspunkte für einen Angriff auf die Sicherheit in der Informationstechnik, der von dem entsprechenden System ausgeht oder zumindest zu erwarten ist. Hierbei wird immer ein Eingriff in die Integrität in das betreffende IT-System vorliegen. Die Gefahr der Tatausführung steht kurz vor Justizvergütungs-/ und -entschädigungsgesetzes der Durchführung, der Schadenseintritt für die zu schützenden Rechtsgüter droht unmittelbar. Beispielsweise kann ein Fernzugriff auf Systeme notwendig werden, z.B. ein Zugriff auf IoT-Geräte zur Installation von lückenschließender Software (Patches),

um einen DDoS-Angriff zu unterbinden. Oder, mittels Installation eigener Software (auf der Grundlage vorheriger Aufklärungsmaßnahmen entwickelt) kann ein Eingriff in einen Steuerungs-Server erfolgen, um ein Botnetz abzuschalten.

So kann die Übernahme bzw. Steuerung des C&C-Servers in einer Botnetz-Infrastruktur der Vorbereitung zum Senden des in der Schadsoftware bereits enthaltenen Deinstallationsbefehls (sog. Kill-Switch) oder zum Senden eines Updates mit geänderten Kommunikationsparametern an die infizierten Bots dienen. Diese kommunizieren anschließend mit einer von der Bundespolizei vorgegebenen Anschlusskennung (sog. Sinkhole). Daneben können Veränderungen an einem IT-System des Angreifers vorgenommen werden, die dazu dienen, einen Angriff direkt abzuwehren, indem z.B. direkte Veränderungen am System in angreiferseitigen Skripten den Angriff aufhalten oder umlenken. Eine Veränderung oder Löschung von Datensammlungen kommt sowohl für technische Daten (der vom Angriff auf die Sicherheit in der Informationstechnik bedrohten IT-Systeme oder Steuerungscodes) als auch abgeschöpfte Dokumente in Frage.

Erfolgt ein DDoS-Angriff auf kritische Infrastruktur (KRITIS) im Aufgabenbereich gemäß § 1 Absätzen 3 bis 6 sowie den §§ 2 bis 8 BPolG über Server in Deutschland, bei dem der zuständige Anbieter nicht zur Abschaltung des entsprechenden Servers verpflichtet werden kann, ist die Bundespolizei nach Absatz 2 befugt, unter Zuhilfenahme von aus einer anderen polizeilichen Maßnahme rechtmäßig erlangten Zugangsdaten auf den Server zugreifen. Dabei können Datenveränderungen des informationstechnischen Systems erforderlich sein, um den Angriff abzuwehren.

Die neue Befugnis gestattet den verdeckten Eingriff auch in informationstechnische Systeme von Geschädigten („Opfersysteme“), von denen ebenso eine Gefahr für die Sicherheit in der Informationstechnik ausgeht. Zum Zweck der Bereinigung dürfen von der Schadsoftware Konfigurationsdaten verändert und gelöscht werden.

Aufgrund der Schwere des Eingriffs solcher Maßnahmen, wird nach Satz 1 vorausgesetzt, dass die betroffenen Systeme zur Verwirklichung einer Straftat nach § 41a Absatz 1 verwendet werden oder verwendet werden sollen und von ihnen eine dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt oder für die Vertraulichkeit oder die Integrität informationstechnischer Systeme einer großen Anzahl von Personen, ausgeht.

Ferner muss nach Satz 2 als besondere Ausprägung des Verhältnismäßigkeitsgrundsatzes die Voraussetzung vorliegen, dass die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Satz 3 verweist auf die entsprechende Geltung der Regelungen von § 41a Absatz 1 Satz 2 bis 4 gelten entsprechend.

Zu Absatz 2

Nach Absatz 2 ergeht die gerichtliche Anordnung über die Maßnahme nach 41b Absatz 1 auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung. Bei Gefahr im Verzug kann die Anordnung durch ebendiese selbst getroffen werden, wobei eine gerichtliche Entscheidung binnen drei Tagen nachzuholen ist.

Zu Absatz 3

Verarbeitungsregelung von erhobenen Daten nach Absatz 1 und 3.

Zu Absatz 4

Als weitere Ausprägung des Verhältnismäßigkeitsgrundsatzes schreibt Absatz 4 in Bezug auf Maßnahmen nach Absatz 2 zur Mitigierung der Eingriffsintensität vor, dass nur solche Veränderungen vorzunehmen sind, die unerlässlich zur Erhebung, Löschung und Veränderung der Daten sind und dass diese soweit möglich automatisiert rückgängig zu machen sind, soweit dies technisch möglich ist.

Insbesondere ist die auf dem IT-System installierte Software vollständig zu löschen und sind Veränderungen an den bei der Installation der Software vorgefundenen Systemdateien rückgängig zu machen. Die Rückgängigmachung der vorgenommenen Veränderungen hat im Interesse einer möglichst zuverlässigen und einfachen Abwicklung grundsätzlich automatisiert zu geschehen. Soweit eine automatisierte Rückgängigmachung technisch unmöglich ist, sind die vorgenommenen Veränderungen, soweit möglich, manuell rückgängig zu machen.

Zudem ist das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Insbesondere hat die Bundespolizei dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte zweckentfremdet werden kann. Speziell ist sicherzustellen, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von der Bundespolizei verwendeten zurückzumelden, und dass die Software weder von Unbefugten erkannt noch angesprochen werden kann. Dies soll gewährleisten, dass die Eingriffe in die Integrität des IT-Systems und die Vertraulichkeit der in ihm gespeicherten Daten nicht über das hinausgehen, was nötig ist, um der Bundespolizei die Maßnahme zu ermöglichen. Die Verpflichtung, das eingesetzte Mittel „nach dem Stand von Wissenschaft und Technik“ gegen unbefugte Nutzung zu schützen, bedeutet, dass sich die Bundespolizei der fortschrittlichsten technischen Verfahren bedienen muss, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse erforderlich sind. Hierfür muss es die einschlägigen Aktivitäten auf den Gebieten der Wissenschaft und Technik umfassend und sorgfältig beobachten und auswerten. Diese erhöhten Schutzanforderungen tragen

dem besonderen Gewicht des Eingriffs in die Integrität privat oder geschäftlich genutzter IT-Systeme (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07 Absatznr. 200) Rechnung.

Die Vorgaben zum Kernbereichsschutz nach § 41 Absatz 3 Satz 2 bis 6 gelten entsprechend.

Zu § 41c (Einschränkung von IT-Systemen bei Gefahren für die Sicherheit in der Informationstechnik)

Zu Absatz 1

Die Befugnisnorm dient u.a. dem Zweck des Abschaltens krimineller Infrastruktur sowie infizierter Systeme. Dies kann z.B. die Deaktivierung von infizierten Bots oder von C&C-Servern bedeuten. Eine solche Deaktivierung kann durch Verpflichtung oder Inanspruchnahme der relevanten Dienste-anbieter erfolgen.

Entsprechende Maßnahmen können erforderlich sein, wenn z.B. das Eingreifen in oder Löschen auf angreifenden Systemen nicht oder nicht rechtzeitig möglich oder anderweitig nicht erfolgversprechend ist. In dieser Fallkonstellation wäre ein verdeckter Eingriff in das IT-System des Angreifers (in Abgrenzung zu § 41b Absatz 1) zunächst nicht notwendig oder möglich.

Bislang bestand keine gesetzliche Möglichkeit, Provider zum Abschalten von Servern, die im Rahmen eines Angriffs auf die Sicherheit in der Informationstechnik genutzt werden, zu verpflichten. Bisher besteht lediglich die Möglichkeit auf Grundlage sog. Abuse-Meldungen unter Verweis auf die Verwendungsweise der durch die Angreifer genutzten Server die Provider zu bitten, diese auf freiwilliger Basis abzuschalten. Da Provider regelmäßig ohne rechtliche Verpflichtung keinerlei Maßnahmen treffen, die in Rechte ihrer Kunden eingreifen, bestand das Risiko, dass Server, die einem Botnetz zugehörig waren sowie durch die Betreiber des Botnetzes angemietete Server online blieben.

Weitere Maßgaben ergeben sich über den Verweis in Satz 2 auf Absatz 2.

Zu Absatz 2

Nach Absatz 2 ergeht die gerichtliche Anordnung über die Maßnahme nach 41c Absatz 1 auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder der Präsidentin oder des Präsidenten der Bundespolizeidirektion oder ihrer oder seiner Vertretung. Bei Gefahr im Verzug kann die Anordnung durch ebendiese selbst getroffen werden, wobei eine gerichtliche Entscheidung binnen drei Tagen nachzuholen ist.

Zu Absatz 3

Absatz 3 legt die Inhalte des Antrags nach Absatz 2 fest. Demnach muss dieser die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, von dem eine Gefahr ausgeht oder auf das der Angriff auf die Sicherheit in der Informationstechnik gerichtet ist, sowie Art, Umfang und Dauer der Maßnahme, den Sachverhalt und eine entsprechende Begründung beinhalten.

Zu Absatz 4

In Absatz 4 sind die erforderlichen Inhalte der Anordnung nach Absatz 2 geregelt. Diese muss die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems enthalten, von dem eine Gefahr ausgeht oder auf das der Angriff auf die Sicherheit in der Informationstechnik gerichtet ist, sowie Art, Umfang, Dauer und Endzeitpunkt der Maßnahme, den Sachverhalt und die wesentlichen Gründe.

Zu Nummer 2

Da die neu geschaffenen §§ 41a, 41b, 41c verdeckte und eingriffsintensive Maßnahmen vorsehen, wird die Regelung der Benachrichtigungspflicht nach § 78 BPolG-neu unterworfen. Zu benachrichtigen sind die von der Maßnahme Betroffenen. Dies können sein: der Nutzer und der Inhaber des informationstechnischen Systems, von dem die Gefahr ausgeht, der Inhaber des informationstechnischen Systems, auf das der Angriff gerichtet ist, der Nutzer und der Inhaber des informationstechnischen Systems, dessen Betrieb eingeschränkt oder unterbunden wurde, der Nutzer, dem der Betrieb des informationstechnischen Systems untersagt wurde.

Zu Nummer 3

Da die neu geschaffenen §§ 41a, 41b, 41c verdeckte und eingriffsintensive Maßnahmen vorsehen, wird die Regelung der Pflicht zur Löschung von durch Besondere Mittel der Datenerhebung oder vergleichbare Maßnahmen erlangten personenbezogenen Daten nach § 81 BPolG-neu unterworfen.

Zu Nummer 4

Da die neu geschaffenen §§ 41a, 41b, 41c verdeckte und eingriffsintensive Maßnahmen vorsehen, wird die Regelung der Vorschrift zur Protokollierung bei Verdeckten und eingriffsintensiven Maßnahmen nach § 85 BPolG-neu unterworfen. Zu protokollieren sind bei Maßnahmen nach §§ 41a, 41b, 41c der Nutzer und der Inhaber des informationstechnischen Systems, von dem die Gefahr ausgeht, der Inhaber des informationstechnischen Systems, auf das der Angriff gerichtet ist, der Nutzer und der Inhaber des informationstechnischen Systems, dessen Betrieb eingeschränkt oder unterbunden wurde.

Zu Nummer 5

Zur Abwehr von schwerwiegenden Gefahren für die Sicherheit in der Informationstechnik kann die Bundespolizei nach §§ 41a, 41c Dritte zur Mitwirkung verpflichten. Um die vorgesehenen Gefahrenabwehrbefugnisse auch rechtlich gegenüber diesen Dritten durchsetzen zu können, ist eine Bußgeldbewehrung erforderlich, damit eine rechtswidrige Offenbarung oder rechtswidrige Nichtmitwirkung sanktioniert werden kann.

Zu Nummer 6

Da die neu geschaffenen §§ 41a, 41b, 41c verdeckte und eingriffsintensive Maßnahmen vorsehen, wird die Regelung der Berichtspflicht gegenüber dem Deutschen Bundestag nach § 107 BPolG-neu unterworfen.

2. Haftantragsbefugnis Abschiebehaft für Inlandsfälle:

Ergänzung **§ 71 AufenthG:**

„(3a) Ungeachtet der Zuständigkeit nach Absatz 3 ist die Bundespolizei für Abschiebungen und Zurückschiebungen von Drittstaatsangehörigen zuständig, sofern

1. *diese im Zuständigkeitsbereich der Bundespolizei festgestellt wurden,*
2. *diese vollziehbar ausreisepflichtig sind,*
3. *deren Abschiebung nicht oder nach § 60a Absatz 2 Satz 1 Alternative 1 insbesondere aufgrund von fehlenden Reisedokumenten ausgesetzt ist und nach Einschätzung der Bundespolizei die notwendigen Reisedokumente innerhalb von sechs Monaten beschafft werden können und*
4. *das Einvernehmen mit der zuständigen Ausländerbehörde hergestellt wurde.*

Kann, insbesondere außerhalb der üblichen Geschäftszeiten der zuständigen Ausländerbehörde, das Einvernehmen nach Satz 1 Nummer 4 nicht sofort hergestellt werden, ist dies unverzüglich nachzuholen. Die Bundespolizei ist berechtigt, unaufschiebbare Maßnahmen, insbesondere die Beantragung von Haft zur Sicherung der Abschiebung, zu treffen. Die Zuständigkeit der Bundespolizei nach Satz 1 endet, wenn

1. *im Falle der Aussetzung der Abschiebung aufgrund von fehlenden Reisedokumenten nicht innerhalb von sechs Monaten nach der Feststellung des Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei die Beschaffung von Reisedokumenten gelungen ist und eine Beschaffung nicht unmittelbar bevorsteht,*

2. *nach Feststellung des Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei andere rechtliche oder tatsächliche Gründe aufgetreten sind oder fortbestehen, die einer Abschiebung innerhalb von sechs Monaten nach der Feststellung entgegenstehen oder*
3. *die zuständige oberste Landesbehörde der Bundespolizei mitteilt, dass die Zuständigkeit wieder von der Ausländerbehörde wahrgenommen werden soll.*

Absatz 3 Nummer 1e und 2 gilt in den Fällen des Satzes 1 entsprechend."

Begründung:

Von § 71 Absatz 3a AufenthG umfasst sind lediglich vollziehbar ausreisepflichtige Drittstaatsangehörige, die sich entweder im Bundesgebiet ohnehin unerlaubt aufhalten oder die eine Duldung aufgrund von fehlenden Reisedokumenten erhalten haben.

In diesen Fällen soll die Bundespolizei einen Haftantrag stellen können, damit die Person nicht mit einer Anlaufbescheinigung auf freien Fuß gesetzt werden muss. Die Bundespolizei würde dann unverzüglich die Beschaffung von ggf. erforderlich Passersatzpapieren priorisiert angehen und dafür ihre guten Kontakte zu Drittstaaten nutzen und ihre eigenen, dort eingesetzten Dienstkräfte in die Beschaffung einbinden.

Außerdem ist das Tätigwerden durch die Bundespolizei an die Herstellung des Einvernehmens mit der zuständigen Ausländerbehörde geknüpft. Kann, insbesondere außerhalb der üblichen Geschäftszeiten der zuständigen Ausländerbehörde (z.B. an Wochenenden, an Feiertagen oder nachts), dieses Einvernehmen nicht sofort hergestellt werden, muss es unverzüglich nachgeholt werden; bis dahin ist die Bundespolizei berechtigt, unaufschiebbare Maßnahmen zu treffen, beispielsweise die Beantragung von Haft zur Sicherung der Abschiebung nach § 62 Absatz 3 und 5 AufenthG.

Im Übrigen ist die Bundespolizei bereits jetzt für Abschiebungen und Haftanträge zuständig, wenn ein Drittstaatsangehöriger unerlaubt einreist und in irgendeinem Grenzgebiet durch die Bundespolizei festgestellt wird, selbst dann, wenn er quer durch das Bundesgebiet gereist ist (sog. Transitfall). Die Kompetenz für Abschiebungen und Haftsachen ist bereits vorhanden.

Als eine Lehre aus dem Anschlag auf den Berliner Weihnachtsmarkt am 19. Dezember 2016 sollen insbesondere durch § 71 Absatz 3a AufenthG zuständigkeitsbedingte Brüche im Bearbeitungsprozess durch Schnittstellenreduzierung vermieden werden.

Satz 2 legt fest, dass die Zuständigkeit der Bundespolizei auf maximal sechs Monate begrenzt ist. Sie endet, wenn die Abschiebung (z.B. mangels erfolgreicher Passersatzbeschaffung) in diesem

Zeitraum nicht gelingt und dies in absehbarer Zeit auch nicht zu erwarten ist oder, wenn nachträglich tatsächliche oder rechtliche Hindernisse auftreten, die der Abschiebung innerhalb von sechs Monaten nach der Feststellung der Drittstaatsangehörigen im Zuständigkeitsbereich der Bundespolizei entgegenstehen. Nach diesem Zeitraum lebt die Zuständigkeit der bisher befassten Aufenthaltsbehörde wieder auf.

3. Strafverfolgungszuständigkeit der Bundespolizei für einige weitere Verbrechen und auf staatsanwaltlichen Antrag (sog. gekorene Zuständigkeit)

Im Gesetzentwurf bedarf es darüber hinaus zusätzlich der Ergänzung des § 13 BPolG (Verfolgung von Straftaten), **die Änderungen sind grau hinterlegt.**

§ 13 BPolG - Verfolgung von Straftaten

(1) Die Bundespolizei nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung (§§ 161, 163 der Strafprozessordnung) wahr, sofern der Verdacht eines Vergehens (§ 12 Absatz 2 des Strafgesetzbuches) besteht, das

1. *gegen die Sicherheit der Grenze oder die Durchführung ihrer Aufgaben nach § 2 gerichtet ist,*

2. *nach den Vorschriften des Passgesetzes, des Aufenthaltsgesetzes, des Asylgesetzes oder des Freizügigkeitsgesetzes/EU zu verfolgen ist, soweit es durch den Grenzübertritt oder in unmittelbarem Zusammenhang mit diesem begangen wurde,*

3. *einen Grenzübertritt mittels Täuschung, Drohung, Gewalt oder auf sonst rechtswidrige Weise ermöglichen soll, soweit es bei der Kontrolle des grenzüberschreitenden Verkehrs festgestellt wird,*

4. *das Verbringen einer Sache über die Grenze ohne behördliche Erlaubnis als gesetzliches Tatbestandsmerkmal der Strafvorschrift verwirklicht, sofern der Bundespolizei durch oder auf Grund eines Gesetzes die Aufgabe der Überwachung des Verbringungsverbotes zugewiesen ist,*

5. *auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes begangen wurde und gegen die Sicherheit eines Benutzers, der Anlagen oder des Betriebes der Bahn gerichtet ist oder das Vermögen der Bahn oder ihr anvertrautes Vermögen betrifft,*

6. dem deutschen Strafrecht unterliegt und Strafverfolgungsmaßnahmen auf See seewärts des deutschen Küstenmeers im Rahmen des § 7 Satz 1 und 3 erforderlich macht.

7. gegen die Sicherheit der Anlagen oder des Betriebes des Luftverkehrs gerichtet ist und im Zuständigkeitsbereich der Bundespolizei festgestellt wird.

Darüber hinaus nimmt die Bundespolizei die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung auch wahr, soweit der Verdacht eines Verbrechens (§ 12 Absatz 1 des Strafgesetzbuches) besteht

1. nach Satz 1 Nummer 2,

2. nach Satz 1 Nummer 5, soweit ein Verdacht nach 244a, 249, 250, 252, 255 oder 308 Absatz 1 oder § 315 Absatz 3 des Strafgesetzbuches besteht,

3. in Fällen von Satz 1 Nummer 6 und Nummer 7, insbesondere § 315 Absatz 3 und § 316c des Strafgesetzbuches.

(2) Die Bundespolizei ist vorbehaltlich besonderer gesetzlicher Zuständigkeitsregelungen für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung in den Fällen des Absatzes 1 örtlich zuständig, wenn die Straftat in ihrem räumlichen Zuständigkeitsbereich (§ 1 Absatz 8) begangen wurde. Im Übrigen bleibt die Zuständigkeit anderer Polizeibehörden für die Strafverfolgung auch in den Fällen des Absatzes 1 unberührt. Die Staatsanwaltschaft kann im Benehmen mit der Bundespolizei die Ermittlungen einer anderen sonst zuständigen Polizeibehörde übertragen

(3) Bei Straftaten, die nicht dem Absatz 1 unterfallen, ist der Ermittlungsvorgang unverzüglich an die zuständige Strafverfolgungsbehörde abzugeben. Die Verpflichtung der Bundespolizei nach § 163 Absatz 1 der Strafprozessordnung, alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten, bleibt unberührt. Die Sätze 1 und 2 gelten für Straftaten im Sinne des Absatzes 1 entsprechend, wenn diese im Zusammenhang mit weiteren Straftaten stehen und das Schwergewicht der Straftaten insgesamt außerhalb der Zuständigkeit der Bundespolizei liegt oder wenn bei Straftaten seewärts des deutschen Küstenmeers nach Absatz 1 Satz 1 Nummer 6 oder Absatz 1 Satz 2 Nummer 3 Ermittlungshandlungen im deutschen Hoheitsgebiet erforderlich sind. Die Staatsanwaltschaft kann in Zweifelsfällen die zuständige Polizeibehörde bestimmen.

(3a) Bei Straftaten, die nicht dem Absatz 1 unterfallen, nimmt die Bundespolizei abweichend von Absatz 3 die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr, wenn eine Staatsanwaltschaft darum ersucht. Die für die Strafrechtspflege und die Polizei zuständigen obersten Landesbehörden sind unverzüglich zu benachrichtigen, wenn die Bundespolizei polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung wahrnimmt; außerdem sind unverzüglich

zu benachrichtigen die zuständigen Landeskriminalämter, der Generalbundesanwalt in den Fällen, in denen er für die Führung der Ermittlungen zuständig ist, und in den übrigen Fällen die Generalstaatsanwaltschaften, in deren Bezirk ein Gerichtsstand begründet ist. Satz 1 Nummer 1 gilt entsprechend für die Fahndung nach Verurteilten zum Zwecke der Vollstreckung.

(4) Sind Ermittlungshandlungen außerhalb der in § 1 Absatz 8 bezeichneten Bereiche erforderlich, trifft die Bundespolizei ihre Maßnahmen im Benehmen mit der Polizei des Landes.

(5) Die Beamtinnen und Beamten im Polizeivollzugsdienst der Bundespolizei, die mindestens vier Jahre dem Polizeivollzugsdienst angehören, sind Ermittlungspersonen der Staatsanwaltschaft (§ 152 des Gerichtsverfassungsgesetzes) und haben die Rechte und Pflichten der Polizeibeamtinnen und der Polizeibeamten nach der Strafprozessordnung. In den Fällen des Absatzes 1 Nummer 6 gelten auf See seewärts des deutschen Küstenmeers bei der Verfolgung von Straftaten zur Erfüllung völkerrechtlicher Verpflichtungen oder zur Wahrnehmung völkerrechtlicher Befugnisse die Vorschriften der Strafprozessordnung entsprechend.

Begründung:

Zu Absatz 1:

In Bezug auf die Zuständigkeit der Bundespolizei für polizeiliche Maßnahmen auf dem Gebiet der Strafverfolgung wird die bisher bestehende grundsätzliche Beschränkung auf Vergehen beibehalten, jedoch um einige weitere Verbrechen ergänzt. Diese Änderung liegt maßgeblich darin begründet, dass sich die nach dem bisherigen BPolG bestehende Unterscheidung zwischen Vergehen und Verbrechen als nicht zweckmäßig erwiesen hat, sondern verschiedene Zuständigkeiten vielmehr oftmals zu einem künstlichen Aufspalten eines einheitlichen Lebenssachverhalts führten. Dies wurde besonders deutlich in Sachverhalten, in denen zunächst wegen des Verdachts eines Vergehens ermittelt wurde und sich im Laufe der Ermittlungen ein Verdacht eines Verbrechens ergab, sich zum Beispiel der gewerbsmäßige Taschendiebstahl auf dem Bahnhof gemäß § 243 Absatz 1 Satz 2 Nummer 3 Strafgesetzbuch (Vergehen) später als bandenmäßiger gewerbsmäßiger Diebstahl nach § 244a Absatz 1 in Verbindung mit § 243 Absatz 1 Satz 2 Nummer 3 Strafgesetzbuch (Verbrechen) darstellte. Insoweit ergeben sich bislang ermittlungshindernde Schnittstellen in Fällen, in denen nach Durchführung möglicherweise eines Großteils der Ermittlungen aufgrund eines weiteren hinzutretenden Umstandes (Bande) die Abgabe der Ermittlungen an die neu zuständige Behörde erforderlich wird. Derartige Schnittstellen gilt es künftig zu vermeiden.

Auch im Übrigen scheint es aus polizeitaktischen Gründen sachgerecht, ein paralleles Ermitteln mehrerer Behörden innerhalb eines deliktischen Bereichs (z. B. Diebstähle an Bahnhöfen) zugunsten einer verbleibenden Verantwortlichkeit aufzugeben.

Nummer 7 bezieht sich auf Angriffe gegen die Sicherheit und den Betrieb des Luftverkehrs. Umfasst sind insbesondere solche Straftaten, die im Zusammenhang mit Drohnenangriffen verwirklicht werden können (z. B. §§ 315, 316b StGB). Der Bundespolizei sind in diesem Zusammenhang zahlreiche Fälle bekannt, in denen beispielsweise durch fernmanipulierte Luftfahrzeuge (Drohnen) im Bereich von Flughäfen, durch den Einsatz von Lichtzeigern (sog. Laserpointer) gegen im Einsatz befindliche Polizeihubschrauber oder andere, gleichsam gefährliche Eingriffe die Sicherheit des Luftverkehrs beeinträchtigt wurde. Damit korrespondierend normiert § 39 die präventivpolizeiliche Befugnis zur Abwehr von Drohnenangriffen. Eine Einschränkung ergibt sich daraus, dass der Tatverdacht im Zuständigkeitsbereich der Bundespolizei festgestellt worden sein muss.

Zu Absatz 3a:

Die Bundespolizei nimmt über die obligatorischen Fälle des § 13 Absatz 1 hinaus die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr, wenn eine Staatsanwaltschaft darum ersucht. Dabei lässt sich das Ersuchen einer Staatsanwaltschaft des Landes als kompetenzrechtlich unbedenklicher Fall der Amtshilfe begreifen. Insbesondere können länderübergreifende komplexe strafrechtrelevante Sachverhalte unter der Sachleitung der federführenden Staatsanwaltschaft bei einer Ermittlungsbehörde zusammengeführt werden. Beispielhaft aus der Praxis sind grenz- und länderübergreifende Tätergruppierungen, die sich auf Fahrkartenautomatenaufbrüche und -sprengungen, aber auch auf Geldautomatenaufbrüche und -sprengungen in Bahnhofsnähe konzentriert haben. Hierbei kommt zusätzlich die grenz- und bahnpolizeiliche Expertise auch in der Strafverfolgung zum Tragen. Gleiches kann gelten für Straftaten wie z.B. Schleusungskriminalität in Verbindung mit Urkunden- oder sonstiger milieubedingter Kriminalität (u.a. Clanbereiche). Bei nichtfreizügigkeitsberechtigten Staatsangehörigen können zudem nach der Strafvollstreckung Synergieeffekte im Bereich der Rückführung erzielt werden.

Gleichsam kompetenzrechtlich unbedenklich ist die Strafverfolgungstätigkeit der Bundespolizei auf Ersuchen einer Bundesbehörde, beispielsweise wenn der Generalbundesanwalt um Strafverfolgung ersucht oder einen diesbezüglichen Auftrag erteilt. Die Strafverfolgungsaufgabe des Generalbundesanwalts ergibt sich aus Artikel 96 Absatz 5 GG, insoweit kann die Bundespolizei den Generalbundesanwalt als weitere Strafverfolgungsbehörde unterstützen.

4. Sicherheitsforschung in der Bundespolizei

Im Gesetzentwurf bedarf es darüber hinaus zusätzlich der Ergänzung des § 1 Abs. 9 BPolG-E (Allgemeines) zur Erweiterung der Forschungsaufträge auf das gesamte Aufgabenfeld der Bundespolizei.

§ 1 BPolG - Allgemeines

(9) Die Bundespolizei hat zur Erfüllung der Aufgaben nach diesem Gesetz sowie zur Unterstützung der Luftsicherheitsbehörden und der Polizeien des Bundes zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs im Rahmen des § 5 Luftsicherheitsgesetz die erforderliche Einrichtung zur Forschung zu unterhalten.

Begründung:

Zu Absatz 9:

Zur Bewältigung aktueller und zukünftiger Herausforderungen benötigt die Bundespolizei komplexe technische Lösungen, die teilweise nicht im erforderliche Maße am Markt verfügbar sind. Dies betrifft insbesondere zukunftsweisende Sicherheitsausrüstung zum Schutz vor Angriffen auf die Sicherheit des zivilen Luftverkehrs, technische Lösungen zur frühzeitigen Erkennung von Attentätern, Abwehr von Drohnen und Detektion von Tatmitteln, oder etwa den Schutz maritimer Infrastrukturen auf See, Schutzausrüstung für die CBRN-Entschärfter der GSG 9, Unterwasseraufklärungstechnologie oder technischer Lösungen im Bereich non-letaler Wirkmittel.
Neue Tatbegehungsmethoden können Defizite beim derzeitigen Stand der Technik aufzeigen und eine systematische wissenschaftliche Lösungssuche erfordern.

Hierzu ist eine Einrichtung mit hinreichender Ausstattung an Personal und Haushaltsmitteln zu unterhalten. Um eigene Forschungsprojekte auch als Projektträger initiieren zu können, sollte bereits jetzt eine umfassende gesetzliche Grundlage im neunen Bundespolizeigesetz geschaffen werden. Dies kann ganz einfach mit der Erweiterung des § 1 BPolG um den erweiterten Absatz 9 erfolgen.