

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Frank Tempel,
Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/8356 –**

Funktionsweise des Informationsaustauschs zwischen Polizeibehörden in Deutschland

Vorbemerkung der Fragesteller

Im Nachgang zu den terroristischen Anschlägen vom 22. März 2016 in Brüssel wurde im politischen Raum mehrfach die Forderung nach einem Ausbau des Datenaustauschs der Polizeibehörden in den Mitgliedstaaten der Europäischen Union erhoben. So äußerte der Bundesminister des Innern Dr. Thomas de Maizière in den „ARD-Tagesthemen“ noch am Tag der Anschläge, eine Verknüpfung der bislang getrennten „Datentöpfe“ der Sicherheitsbehörden sei nötig. „Datenschutz ist schön, aber in Krisenzeiten hat Sicherheit Vorrang“, führte der Bundesminister im Interview weiter aus.

Es bestehen allerdings schon erhebliche Zweifel, ob ein mehr an Daten und Zugriff auf mehr Datenbanken, die immer auch mit Grundrechtseingriffen einhergehen, überhaupt zu einer verbesserten Gefahrenabwehr führen. So führte Sascha Lobo in einer Kolumne unter dem Titel „Terror und Datenwahn“ auf „SPIEGEL ONLINE“ vom 30. März 2016 aus, dass alle identifizierten Attentäter der einschlägigen Anschläge der letzten zwei Jahre zuvor polizeilich bekannt waren. Auch wird immer wieder darüber berichtet, dass bestehende Möglichkeiten des Informationsaustauschs zwischen den EU-Staaten kaum genutzt werden oder die zugelieferten Daten aufgrund stark abweichender Erfassungssprachen nicht zu belastbaren Lagebildern führen („Warum Europa im Kampf gegen den Terror versagt“, Süddeutsche Zeitung vom 24. März 2016).

Auch bezogen auf die Bundesrepublik Deutschland ist eine kritische Analyse der polizeilichen Aufgabenwahrnehmung erforderlich. Auf dem Internetportal police.it.org, das sich mit der Polizei und ihren Informationssystemen beschäftigt, wurden in einem Beitrag unter der Überschrift „Reine Schaufensterpolitik: De Maizière will ‚ran an die Datentöpfe““ deutliche Zweifel geäußert, ob die Polizei derzeit überhaupt in der Lage ist, ihre bereits bestehenden Befugnisse und Pflichten zur Weitergabe von Daten untereinander nach bestehenden Rechtsgrundlagen wahrzunehmen.

Selbst vom gleichen Anbieter (rola Security Solutions GmbH) beschaffte, so genannte Fallbearbeitungssysteme, die beim Bundeskriminalamt (BKA), der Bundespolizei (dort b-case) und zwei Dritteln der Landeskriminalämter (LKA;

dort RSCase) genutzt würden, seien demnach nicht in der Lage, miteinander Informationen auszutauschen.

Um in der urwüchsig entstandenen IT-Landschaft der deutschen Polizeibehörden überhaupt zu einem digitalen Datenaustausch zu kommen, seien in der Vergangenheit unterschiedliche Lösungen entwickelt worden. Schon seit Jahren existieren zahlreiche, so genannte Verbunddateien, „Datentöpfe“ für spezifische Anwendungsbereiche, in die die Polizeibehörden der Länder und des Bundes Informationen einstellen und im Gesamtbestand suchen können. Die meisten dieser Verbunddateien nutzen das vom BKA selbst (weiter-)entwickelte Informationssystem INPOL-Fall. Seit dem Jahr 2006 stellt das BKA hierfür die Bund-Länder-Datei-Schnittstelle (BLDS) zur Verfügung. Dabei handelt es sich um ein standardisiertes Verfahren, das die IT-Systeme der Teilnehmer (sprich der Länder) nutzen kann, um Informationen aus den Landessystemen elektronisch bei der Verbunddatei im BKA anzuliefern und von dort abzurufen.

Die technischen Schwierigkeiten beim Datenaustausch bestünden jedoch fort. Auch eine von der Innenministerkonferenz im Herbst 2011 beschlossene Anschaffung einer Gemeinsamen Ermittlungsdatei – GED – „Zwischenlösung“, die insbesondere dann zum Einsatz kommen solle, wenn das BKA im Rahmen der Gefahrenabwehr oder der Strafverfolgung im Zusammenhang mit dem internationalen Terrorismus aktiv wird, habe die altbekannten technischen Schwierigkeiten. „Police-it.org“ berichtet unter Bezugnahme auf die Pressestelle des Bundesministeriums des Innern (BMI), dass die GED derzeit nicht über Schnittstellen verfüge, die eine Datenanlieferung aus den Landesfallbearbeitungssystemen erlaube. Dazu müssten eigens installierte Terminals genutzt werden, was zu Doppelarbeit bei den Landesbehörden führe.

Mit der GED sollte ohnehin nur eine Zwischenlösung gefunden werden, so lange die schon im Jahr 2008 beschlossene Schaffung eines „Polizeilichen Informations- und Analyseverbundes“ (PIAV) noch nicht realisiert ist. Dieses neue Verbundsystem PIAV hinkt den Planungen weit hinterher. Mit den Vorarbeiten war bereits im Jahr 2007 begonnen worden. PIAV soll den Informations- und Nachrichtenaustausch zwischen Polizeibehörden des Bundes und der Länder verbessern und erweitern: Anders als bei bisherigen Verbundlösungen sollen auch solche Informationen untereinander geteilt werden, die im Rahmen der polizeilichen Gefahrenabwehr bzw. noch vor dem Abschluss eines strafrechtlichen Ermittlungsverfahrens erhoben und erfasst werden. Dazu sollen die PIAV-Teilnehmersysteme über ein standardisiertes Verfahren und auf der Basis des von allen einheitlich verwendeten, gemeinsamen Informationsmodells Polizei (IMP) Informationen beim PIAV-Zentralsystem im BKA anliefern sowie dort bearbeiten und recherchieren können. Außerdem soll es möglich sein, Informationen und Nachrichten auch bi- bzw. multilateral zwischen einzelnen PIAV-Teilnehmern auszutauschen. Der Auftrag für das Zentralsystem PIAV Operativ Zentral wurde an das Unternehmen rola Security Solutions GmbH vergeben. Die Inbetriebnahme einer ersten, funktional und fachlich auf den Bereich der Waffen- und Sprengstoffdelikte beschränkten Ausbaustufe von PIAV ist nach Angaben der Bundesregierung gegenüber dem Haushaltsausschuss des Deutschen Bundestages dennoch erst für „Mitte 2016“ geplant, die letzte Ausbaustufe soll im Jahr 2020 mit dem Staatsschutzbereich erreicht werden (<https://police-it.org/schaufensterpolitik-de-maiziere-will-ran-an-die-datentoeffe-11031>).

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 6 in offener Form ganz oder teilweise nicht erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie

Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Behörden und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen.

Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu den technischen Fähigkeiten und nachrichtendienstlichen Verfahrensweisen der Behörden. Aus ihrem Bekanntwerden könnten Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Nachrichtendienstbehörden gezogen werden. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen zur Frage 6 als Verschlussache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlussachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft.

1. Zu bzw. nach welchen Ereignissen wurde in diesem Jahr und in den vergangenen beiden Jahren die GED „Zwischenlösung“ genutzt?

Bisher wurde die Gemeinsame Ermittlungsdatei-Zwischenlösung (GED) nur in einem BKA-Ermittlungsverfahren (Bundeskriminalamt) aus dem Bereich PMK-Rechts genutzt.

- a) Aus welchen der am jeweiligen Verfahren beteiligten Ländern erfolgte die Dateneingabe
 - via eigens installierter GED-Terminals bzw.
 - via direkter elektronischer Schnittstelle zwischen Landessystem und GED-System bzw.
 - mit anderen Verfahren (z. B. Übermittlung von Informationen via Email, Fax oder E-POST)?

Eine Datenerfassung in dem BKA-Ermittlungsverfahren erfolgte durch die Bundesländer Sachsen, Bayern und Rheinland-Pfalz durch Eingabe über GED-Terminals.

- b) Trifft es zu, dass das Zentralsystem der GED „Zwischenlösung“ beim BKA nicht über eine Schnittstelle verfügt, die gegenüber den Ländern offengelegt ist und somit die Entwicklung einer Prozedur zur elektronischen Anlieferung von Informationen bei der GED ermöglicht?

Die GED-„Zwischenlösung“ verfügt über keine gegenüber den Ländern offene Schnittstelle.

- c) Wie hoch war das Aufkommen an Meldungen an die GED durch die Länder anteilig pro Ereignis bzw. über sämtliche Einsatzfälle der GED in diesem Zeitraum?

Die Erhebung der konkreten Anzahl der erfassten Meldungen durch die Länder anteilig pro Ereignis in dem in der Antwort zu Frage 1 genannten BKA-Ermittlungsverfahren ist in der kurzen Frist nicht möglich gewesen.

2. Welche Kosten sind für die Entwicklung der GED angefallen, wer waren bzw. sind die Auftragnehmer für Entwicklung, Beratungsleistungen, Anschluss an die bestehende EDV-Infrastruktur des BKA und laufende Kosten für die Wartung (bitte mit jeweiliger Art der Auftragsvergabe und Kosten auflisten)?

Nachfolgende Auflistung zeigt gemäß Projektabschlussbericht der Gemeinsame Ermittlungsdatei Großschadenslage – TE (GED)-Zwischenlösung auf Basis b-case die Kosten zuzüglich der Wartung auf.

Beschreibung und Basis	Ausgaben in EUR	Kostenzuordnung
HP Infrastruktur	350.961,94	Hardware
Citrix Lizenzen	218.048,78	Lizenzkosten
Netzwerkkabel	3.457,47	Hardware
ServerPass Standard Zertifikate	1.285,20	Zertifikatskosten
Erwerb von zwei weiteren Datenbankinstanzen - Lizenzen für rs-Case Software für GED	23.800,00	Lizenzkosten
Ausweitung der Nutzungsberechtigung b-case für GED	1.000.000,00	Lizenzkosten
Zusatzmodul rsC-623: Info- u. Störungsanzeige in der PIA	8.925,00	Lizenzkosten
Modul BLDS-Schnittstellenadministration	59.500,00	Lizenzkosten
Wartung der Ausweitung der Nutzungsberechtigung b-case für GED (Rola)	580.833,33	Wartung
Wartung Citrix - Lizenzen	48.132,41	Lizenzkosten
Gesamtkosten	2.294.944,13	

Eine weitere Aufschlüsselung nach Vergabeverfahren und Auftragnehmern war in der gegebenen Frist nicht möglich.

3. Bei welchen der einschlägigen terroristischen Großlagen der vergangenen zwei Jahre im Aus- und Inland (insbesondere den Anschlägen in Paris im Januar und November 2015, den Anschlägen in Brüssel, der Länderspielabsage in Hannover, der Lage in München in der Silvesternacht) war ein entsprechender „BAO-Lagefall“ ausgerufen mit der Folge, dass einschlägige Informationen aller Behörden in entsprechenden Verbunddateien zu melden waren?

Das BKA hat in den vergangenen zwei Jahren im Zusammenhang mit den Anschlägen in Paris einen BAO-Lagefall ausgerufen (BAO Paris).

- a) Welche Verbunddatei (BAO-Lagefall o. Ä.) wurde jeweils für den Informationsaustausch entsprechender relevanter Informationen genutzt?

Zur Abbildung und Bearbeitung von Hinweisen im Zusammenhang mit den Anschlägen in Paris/Brüssel steht eine INPOL-Fall-Anwendung mit der Bezeichnung „Einsatzlage Paris/Brüssel“ zur Verfügung.

- b) Wie erfolgte in diesen Fällen ein Informationsaustausch zwischen Ländern und Bund, wenn im Einzelfall kein BAO-Lagefall ausgerufen wurde?

Die Übermittlung relevanter Hinweisinformationen zur Bewältigung einer polizeilichen AAO- oder BAO-Lage erfolgt außerhalb eines ausgerufenen BAO-Lagefalls auf konventionellem Weg unter Beachtung von Datenschutz- und Geheimschutzaspekten, mittels E-Mail, E-Post810, VS-Mail und ElcroDat.

- c) Welche Teilnehmerbehörden haben Informationen elektronisch via BLDS angeliefert?

Die Bundesländer Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und Schleswig Holstein nutzen die Möglichkeit zur Übermittlung von Daten per BLDS.

- d) Wie erfolgte die Anlieferung von Informationen von solchen Teilnehmerbehörden, die nicht die BLDS genutzt haben?

Für alle anderen Bundesländer besteht die Möglichkeit zur manuellen Erfassung über eine bereitgestellte Eingabemaske.

- e) Wie gestaltet sich in diesem Fall das Verfahren der Informationserfassung, -aufbereitung, -übermittlung an das BKA, ggf. die erneute Erfassung und Einspeicherung im Zielsystem?

Die Daten werden in den Quellsystemen der Bundesländer manuell erfasst und per Schnittstelle an das Zielsystem (BAO-Lagefall) angeliefert. Bundesländer ohne diese Möglichkeit erfassen die Daten manuell über eine zentral bereitgestellte Eingabemaske im Zielsystem.

- f) Von welchem Datum stammen die Errichtungsanordnung(-en) zu den entsprechend der Frage 3a genutzten Verbunddatei(-en)?

Die Errichtungsanordnung ist auf den 14. Dezember 2015 datiert.

4. Welche Verfahren der Informationsanlieferung bei der BKA-Zentralstelle wurden seitens der Länderpolizeibehörden und der beiden Bundespolizeibehörden zwischen dem Jahr 2013 und heute tatsächlich praktisch im dauerhaften Wirkbetrieb genutzt zur Anlieferung von Informationen

- a) bei der vom BKA geführten Antiterrordatei (ATD),

Die Fragen 4 und 4a werden gemeinsam beantwortet.

Die Datenanlieferung an die Antiterrordatei (ATD) erfolgt entweder automatisiert per Schnittstelle über die Fallbearbeitungssysteme INPOL-Fall, KRISTAL und b-case (Landeskriminalämter, BKA) oder direkt über die ATD-Oberfläche (Berlin, Niedersachsen, Zollkriminalamt [ZKA] und Bundespolizei [BPOL]). Über die ATD-Oberfläche werden außerdem durch alle Polizeibehörden solche Daten in die ATD übertragen, deren Geheimhaltungsgrad höher als „Verschlusssache - Nur für den Dienstgebrauch“ (VS-NfD) liegt.

b) bei der vom BKA geführten Rechtsextremismusdatei (RED),

Die Datenanlieferung an die Rechtsextremismus-Datei (RED) erfolgt analog zu dem in der Antwort zu Frage 4a dargestellten Verfahren, allerdings ist das ZKA nicht an der RED beteiligt.

c) bei den zentral vom BKA gehosteten Verbunddateien BAO-Lagefall, Streugut, FUSION, DOK Europa-Ost (DOK-DEO) und IFIS (bitte einzeln ausführen)?

Zu den zentral vom BKA gehosteten Verbunddateien „BAO-Lagefall“, „Streugut“, „Fusio“ und „DEO“ kann die Anlieferung von Informationen sowohl über die BLDS-Schnittstelle als auch manuell über eine zentral bereitgestellte Eingabemaske erfolgen. Die Verbunddatei „IFIS“ wird nur manuell bereitgestellt.

5. Welches Verfahren zum Informationsaustausch wurde im Zeitraum von 2013 bis heute in welchen Fällen tatsächlich praktisch genutzt für den Informationsaustausch zwischen Ländern und Bund im Fall einer Großschadenslage im Sinne der Anwendung GSL?

Die Anwendung GSL steht zur Abbildung von Informationen im Zusammenhang mit Großschadenslagen zur Verfügung und bietet Bund und Ländern die Möglichkeit, Daten manuell oder per BLDS zu erfassen. Im Zeitraum 2013 bis heute ist die Anwendung nicht zum Informationsaustausch zwischen Bund und Ländern im Rahmen einer Großschadenslage eingesetzt worden.

6. Welche vertraglichen Möglichkeiten der Einsichtnahme und Prüfung des Quellcodes für die Anwendungskomponenten auf den Clients als auch für die Serverkomponenten stehen den beschaffenden Bundesbehörden zu für die bei dem Unternehmen rola Security Solutions GmbH beschafften Informationssysteme (z. B. RSFrame) und Fallbearbeitungssysteme (z. B. RSCase bzw. b-case) und die auf dieser Basis betriebenen Informationssysteme von Sicherheitsbehörden des Bundes (Zentralsystem für das Nachrichtendienstliche Informationssystem NADIS-neu beim Bundesamt für Verfassungsschutz, Zentralsystem für PIAV Operativ Zentral, für die GED und die ATD beim BKA, Fallbearbeitungssystem b-case für BKA und Bundespolizei)?

Im BKA sind derzeit zwei Systeme der Firma Rola im Einsatz: Das Fallbearbeitungssystem b-case (inkl. GED) und das Zentralsystem PIAV-Z.

Beim Fallbearbeitungssystem b-case ist im Rahmenvertrag für BKA und BPOL eine Regelung zur Nutzung des Quellcode in folgenden Fällen enthalten:

- „über das Vermögen der Auftragnehmerin die Eröffnung des Insolvenzverfahrens beantragt wird,
- über das Vermögen der Auftragnehmerin das Insolvenzverfahren eröffnet wird,
- ein Antrag auf Eröffnung des Insolvenzverfahrens über das Vermögen der Auftragnehmerin mangels Masse abgewiesen wird.“

Weitere Möglichkeiten der Einsichtnahme und Prüfung des Quellcodes wurden im Rahmenvertrag nicht vereinbart. Der Quellcode zu b-case ist im BKA hinterlegt.

Für PIAV-Operativ Zentral musste der Auftragnehmer vertraglich garantieren, dass die Software u. a. frei von nicht in der Programmbeschreibung der Software

beschriebenen Funktionalitäten ist, die geeignet sind, die Integrität, Vertraulichkeit und Verfügbarkeit der Software, anderer Soft- und/oder Hardware insbesondere der Systemumgebung zu gefährden. Darüber hinaus ist vertraglich festgelegt, dass eine Untersuchung des Quellcodes veranlasst werden kann. Der Quellcode zu PIAV-Operativ Zentral ist im BKA hinterlegt.

Das System ATD (sowie auch RED) sind Fachverfahren, die BKA-intern entwickelt wurden und gepflegt werden. Daher ist die Mitwirkung von Fremdfirmen bei Betrieb bzw. Aktualisierung dieser Verfahren nicht notwendig.

- a) Wurden solche Einsichtnahmen und Prüfungen in der Vergangenheit bereits durchgeführt, und wenn ja, wann, und durch wen?
- b) Welcher Änderungs-, Korrektur- und Erweiterungsbedarf ergab sich in Folge solcher Prüfungen?
- c) Welche Behörden des Bundes sind in diese Prüfungen eingebunden bzw. eingebunden gewesen?

Die Fragen 6a bis 6c werden wegen des Sachzusammenhangs gemeinsam beantwortet. Bisher wurde eine entsprechende Einsichtnahme nicht getätigt.

Darüber hinaus wird auf den „VS-Nur für den Dienstgebrauch“ eingestuftem Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

7. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung angesichts der aktuell vorliegenden Erfahrungen mit dem polizeilichen Informationsaustausch aus dem Vorschlag des Bunds Deutscher Kriminalbeamter e. V. (BDK), „die im Grundgerüst bereits bestehende GED entsprechend für die Nutzung für Länder, welche beim BKA hosten möchten, auszubauen“ und damit die landeseigenen Fallbearbeitungssysteme zu ersetzen (siehe www.bdk.de/der-bdk/aktuelles/artikel/polizeiliche-it-landschaft-gleicht-einem-flickenteppich)?

Konkrete Anforderungen der Bundesländer an das BKA in dieser Zielrichtung liegen hier nicht vor.

8. Sind der Bundesregierung andere IT-Systeme/-Produkte im Einsatz von Sicherheitsbehörden des Bundes bekannt, in denen der Hersteller an unterschiedliche Bedarfsträger miteinander nicht kompatible Versionen der gleichen Software ausliefert, sodass Schwierigkeiten beim Austausch von Informationen bestehen?
 - a) Wenn ja, welche IT-Systeme/-Produkte und Hersteller?
 - b) Inwiefern kann man dabei ein ökonomisches Interesse der Hersteller unterstellen, bei der öffentlichen Hand auf diesem Weg weitere Aufträge für die notwendige Programmierung von Schnittstellen zwischen ihren eigenen IT-Systemen und -Produkten zu generieren?
 - c) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus diesem Umstand für den Aufbau eigener Fähigkeiten und Ressourcen für das Controlling von IT-Beschaffungsmaßnahmen?
 - d) Hat sich die Bundesregierung mit dieser Problematik im Rahmen der IT-Strategie bzw. der IT-Konsolidierung Bund befasst?

Die Fragen 8a bis 8d werden gemeinsam beantwortet.

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Es sind der Bundesregierung keine von Sicherheitsbehörden des Bundes eingesetzten IT-Systeme/-Produkte bekannt, in denen der Hersteller an unterschiedliche Bedarfsträger miteinander nicht kompatible Versionen der gleichen Software ausliefert, sodass Schwierigkeiten beim Austausch von Informationen bestehen.

Auch bei den rsCase-Systemen besteht entgegen der Vorbemerkung der Fragesteller der Kleinen Anfrage die Möglichkeit eines Datenaustauschs über Ex- und Importfunktionalitäten (z. B. IMP- oder FTS-Ex-und Import).

9. Mit welcher Beschaffungsmaßnahme (bitte Nummer der Auftrags- und Vergabebekanntmachung angeben) wurden für das BKA und die Bundespolizei die für den Einsatz im PIAV notwendigen Erweiterungen bzw. Zusätze (z. B. Schnittstellen) des bei den beiden Bundespolizeibehörden eingesetzten Fallbearbeitungssystems b-case beauftragt, die in der Leistungsbeschreibung für den veröffentlichten Rahmenauftrag für das System PIAV Operativ Zentral nicht, z. B. als gesondertes Los, enthalten sind und daher durch diesen Rahmenvertrag nicht abgedeckt sein können?

Die Beschaffung der Erweiterungen bzw. Zusätze (z. B. Schnittstellen) von b-case im BKA und in der BPOL erfolgte über den bestehenden Rahmenvertrag zum Betrieb und Weiterentwicklung des Software-Produktes „rsCase“ (B2.60-1946/11 VV:1).

Dieser umfasst im Hauptsächlichen die Weiterentwicklung des Fallbearbeitungssystems entsprechend kundenspezifischer Anforderungen. Ein gesondertes Vergabeverfahren für die Weiterentwicklung des Fallbearbeitungssystems von BPOL und BKA war somit nicht notwendig.

10. Wann rechnet die Bundesregierung mit der Aufnahme des Wirkbetriebs für die erste Ausbaustufe von PIAV-Operativ für Waffen- und Sprengstoffdelikte?

Am 2. Mai 2016 hat PIAV Stufe 1 „Waffen- und Sprengstoffkriminalität“ planmäßig den Wirkbetrieb aufgenommen. Bis zum 10. Mai 2016 wurden sukzessive alle 19 PIAV-Teilnehmer zugeschaltet. PIAV befindet sich bis zum 30. Juni 2016 noch in einer Stabilisierungsphase, um frühzeitig auf ggf. auftretende Fehler in der Anfangszeit reagieren zu können.

11. Welche weiteren Deliktsbereiche sollen über PIAV-Operativ abgedeckt werden, und für wann ist nach derzeitigem Stand mit der Aufnahme des Wirkbetriebs für die entsprechenden PIAV-Ausbaustufen zu rechnen (bitte einzeln auflisten)?

Die derzeitige Planung von PIAV-Operativ sieht nachfolgende Deliktsbereiche vor, die in Stufen bis zum Jahr 2020 umgesetzt werden:

- Waffen- und Sprengstoffkriminalität
- Rauschgiftkriminalität
- Gewaltdelikte/Gemeingefährliche Straftaten
- Eigentumskriminalität und Vermögensdelikte
- Sexualdelikte
- Cybercrime
- Dokumentenkriminalität

- Schleusung/Menschenhandel/Sexuelle Ausbeutung
- Korruption
- Arzneimittelkriminalität
- Falschgeldkriminalität
- Wirtschaftskriminalität / Umwelt- und Verbraucherschutzdelikte
- Geldwäsche
- Organisierte Kriminalität
- Politisch motivierte Kriminalität.

Der Start des Wirkbetriebs für die 2. Stufe des PIAV mit den Dateien „Gewaltdelikte/Gemeingefährliche Straftaten“ und „Rauschgiftdelikte“ ist für Ende 2017 geplant. Die weitere Realisierung ist noch nicht konkret terminiert.

12. Wird der Aufbau der Komponente PIAV-Strategisch und der Module Lagebildmodul und Früherkennungsmodul ebenfalls weiterverfolgt, und wie sieht die Planung zur Konzeption, Entwicklung und Vorbereitung des Wirkbetriebs und des Wirkbetriebs nach derzeitigem oder dem letzten bekannten Stand aus?

Die Konzeption von PIAV sieht eine operative und eine strategische Komponente vor. Insbesondere zur Risikominimierung haben sich Bund und Länder gemeinsam darauf verständigt, zunächst mit der Realisierung von PIAV-Operativ zu beginnen. Gegenwärtig werden von Bund und Ländern jedoch parallel grundlegende Fragestellungen für PIAV-Strategisch geklärt.

13. Wie und wann erfolgt eine Erfolgskontrolle hinsichtlich der für PIAV definierten Ziele, und wer erhält wann und in welcher Form Kenntnis von den Ergebnissen dieser Überprüfung?

Durch Gremien der Innenministerkonferenz wurden bereits Aufträge zur Evaluation bzw. Erfolgskontrolle zu PIAV-Operativ adressiert. Hierzu wurde eine Bund-Länder-Arbeitsgruppe einberufen. Erste Ergebnisse der Evaluation von PIAV werden ein Jahr nach Wirkbetriebsaufnahme der 1. Stufe erwartet.

14. Existierten Überlegungen oder Planungen für den Fall, dass die mit PIAV beabsichtigten und definierten Ziele nicht bzw. nicht in dem für die innere Sicherheit notwendigen Umfang bzw. dem der aktuellen Bedrohungslage entsprechenden Zeitrahmen erreicht werden, und wenn ja, welche?

Nein. Zurzeit sind keine Indikatoren feststellbar, die diese hypothetische Annahme stützen.

