

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/11130 –**

Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen

Vorbemerkung der Fragesteller

Polizeibehörden beklagen sich über eine immense Zunahme digitaler Datenbestände. Von 2007 bis 2009 hätten sich laut Moritz Aly vom Bundeskriminalamt (BKA) bestehende Datenmengen jährlich verdoppelt, „ab 2010 dann stieg das Aufkommen explosionsartig“ (Vortrag auf der Veranstaltung „Europäischer Polizeikongress“, 14. Februar 2012). Behörden wollen die Informationen zunehmend automatisiert durchforsten und aufbereiten. Auf dem Europäischen Polizeikongress widmete sich ein eigenes Panel einer effektiveren digitalen Informationsverarbeitung. Das BKA stellte dort dessen „Inhaltliche Datenträgerauswertung“ (IDA) vor, die das Amt in Eigenregie entwickelt hat. Die Software erkennt Sprachen, sucht doppelte Einträge, filtert relevante Daten heraus und erstellt die für andere Programme notwendigen Statistiken. Dies wurde kürzlich von der Bundesregierung in der Antwort auf die Schriftliche Frage 19 des Abgeordneten Jan Korte auf Bundestagsdrucksache 17/10925 bestätigt. Die „Inhaltliche Datenträgerauswertung“ visualisiert Zusammenhänge und schlägt Hypothesen vor.

Eine derart automatisierte Strafverfolgung wurde vom BKA auch auf den von Bürgerrechtsgruppen heftig kritisierten Schulungen in Weißrussland vorgeführt (Bundestagsdrucksache 17/10713). Gezeigt wurde „Analyst’s Notebook“ der von IBM aufgekauften Firma i2. Die Firma i2 stellte auf dem letzten Europäischen Polizeikongress „Werkzeuge zur Detailanalyse und Visualisierung von Beziehungen zwischen physischen Merkmalen und allen dazu verfügbaren Informationen“ vor. Die Bundesregierung bestätigt, dass „Analyst’s Notebook“ „Hypothesen“ ausgibt und Zusammenhänge visualisiert. Analyst’s Notebook wurde bislang vom deutschen Polizeizulieferer rola Security Solutions vermarktet. Weitere Analysesoftware wurde mit „InfoZoom“ durch das BKA von der Firma humanIT Software GmbH beschafft.

Auf Ebene der Europäischen Union werden Standards für polizeilich genutzte Informationstechnik erarbeitet. Die Europäische Kommission hat das Forschungsprogramm „Composite“ gestartet, das technologische Veränderungsprozesse von Polizeibehörden in zehn europäischen Ländern erforscht. Auch

die Bundesrepublik Deutschland ist beteiligt. Im August 2012 hatte die EU im dänischen Odense die zweite „European Intelligence and Security Informatics Conference“ (EISIC) ausgerichtet, die sich mit Verfahren der „Social Network Analysis“ und des „Data Mining“ befasste. Für sein „Pre-frontier Intelligence Picture“, das auch auf der intelligenten Auswertung von statistischem Material beruht, forscht auch die Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen (FRONTEX) an Verfahren zum „Text Mining“. FRONTEX nimmt am Forschungsprojekt „OPensource Text Information Mining and Analysis“ (OPTIMA) teil. Das Europäische Polizeiamt (Europol) betreibt eine sogenannte Social Network Analysis, wie sie von IBM verkauft wird, schon länger. Europol nutzt laut der EU-Innenkommissarin Cecilia Malmström ebenso Software von i2 „für Analysen und Datamining“ sowie der Firma Themis „für Textmining“ (Kommissionsdokument E-000171/2012). Eine „akademische Software“ analysiert demnach „Subnetze und Schnittpunkte“.

Problematisch ist, wenn auf diese Weise bislang „unstrukturierte Daten“ aus mehreren Quellen verarbeitet werden. Durch dieses sogenannte Data Mining könnten Ermittler/Ermittlerinnen nach neuen Erkenntnissen suchen, indem Einträge auf „Kreuztreffer“ analysiert werden. Die Definition, ab welcher Eingriffstiefe es sich um ein polizeiliches „Data Mining“ oder eine Rasterfahndung handeln würde, ist allerdings umstritten. Auch über die Funktionalität einer „Vorhersage“ gibt es unterschiedliche Auffassungen. Laut dem Staatssekretär im Bundesministerium des Innern (BMI), Klaus-Dieter Fritsche, nutzen oder testen Bundesbehörden keine „prediktiven Analyseprogramme“ (Antwort der Bundesregierung auf die Schriftliche Frage 13 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 17/10503). Jedoch erklärte der BKA-Vizepräsident Prof. Dr. Jürgen Stock auf Fachkonferenzen, das BKA teste jede auf dem Markt befindliche „prediktive Software“ und berichte hierzu den Landeskriminalämtern.

Dass sich Behörden auf zunehmendes „Data Mining“ vorbereiten, zeigt die Verankerung einer „erweiterten Nutzung“ im „Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus“. Gemeint sind „das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu erkannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten“. Im Gesetzestext heißt es, dass Behörden „Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen“ dürfen. In der Antwort auf die Mündliche Frage 39 des Abgeordneten Andrej Hunko (Plenarprotokoll 17/194) erklärt der Parlamentarische Staatssekretär beim Bundesminister des Innern, Dr. Ole Schröder, die „erweiterte Nutzung“ der „Rechtsextremismusdatei“ sei ab einer nun folgenden Projektphase vorgesehen.

Wenn aber Computer Zusammenhänge zwischen Personen, Sachen und Orten analysieren, bedeutet dies eine grundsätzliche Veränderung der Polizeiarbeit. Der erhoffte „Mehrwert“ unstrukturierter Information stellt eine automatisierte Wissensproduktion durch Polizeien und Geheimdienste dar. Die ohnehin zu beobachtende Verlagerung der Strafverfolgung ins Vorfeld bekommt digitale Schützenhilfe. Indikatoren und Routinen, nach denen die Datenbestände durchsucht werden, folgen der polizeilichen Definition von „Risiken“. Wenn eine Software Personendaten auf etwaige Risiken untersucht, muss deren Funktionsweise, mithin ihr Quellcode, bekannt sein. Dies gilt nicht nur für staatliche Trojaner und Programme zum „Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen“.

Vorbemerkung der Bundesregierung

Die Fragesteller verwenden in dieser Kleinen Anfrage sowie in den in der Vorbemerkung der Fragesteller in Bezug genommenen Anfragen und Fragen Begriffe, welche weder im Recht der Europäischen Union noch im deutschen Recht definiert sind und für die bislang keine speziellen gesetzlichen Regelungen bestehen. Weiterhin werden gesetzlich definierte Begriffe wie bzw. die Rasterfahndung in einem anderen Zusammenhang verwendet („rasternde Analysesoftware“).

Die Bundesregierung weist darauf hin, dass sie bei der Beurteilung der Zulässigkeit von Datenverarbeitungsvorgängen die in den einschlägigen Rechtsvorschriften verwendeten Begrifflichkeiten verwendet. Soweit im allgemeinen Sprachgebrauch der Behörden nicht gesetzlich definierte Begriffe verwendet werden, geschieht dies zur Einordnung im Rahmen von technischen oder organisatorischen Zwecken und hängt vom jeweiligen Kontext ab.

Die Vorbemerkung der Fragesteller enthält zudem Begriffe, welche auch vom Sprachgebrauch der Fachliteratur abweichen.

Zur Vermeidung von Missverständnissen gibt die Bundesregierung folgende Hinweise:

„Data Mining“ ist weder im Recht der Europäischen Union noch im deutschen Recht definiert noch existieren bislang gesetzliche Regelungen über die Zulässigkeit des „Data Mining“. In der Regel werden mit diesem Begriff in erster Linie durch die Privatwirtschaft eingesetzte Verfahren und Methoden bezeichnet, mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege „neues Wissen“ zu generieren.

Der Begriff „Massendaten“ ist dem allgemeinen Sprachgebrauch entnommen und wird von Behörden entweder rein technisch zur Beschreibung des Umfangs von Daten oder fachlich zur Beschreibung des Auswertestandes bzw. der verwendeten Erhebungsgrundlage verwendet. Die automatisierte Verarbeitung von personenbezogenen Daten ist in § 3 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes (BDSG) legaldefiniert als „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen“. Soweit öffentliche Stellen in Deutschland in automatisierter Form personenbezogene Daten erheben, verarbeiten oder nutzen, bestimmt sich die datenschutzrechtliche Zulässigkeit nach den gesetzlich festgelegten Anforderungen, wie sie sich aus dem jeweils anwendbaren bereichsspezifischen Datenschutzrecht und subsidiär aus den Vorschriften des Bundesdatenschutzgesetzes bzw. der Landesdatenschutzgesetze ergeben.

„Prediktive Analyse“ wird in der Fachliteratur allgemein als Verfahren zur Erstellung einer Vorhersage über Ereignisse, Zustände oder Entwicklung in der Zukunft verstanden. Die von den Fragestellern vorgenommene Einengung auf die Vorhersage für das Verhalten von Einzelpersonen wird von der Bundesregierung nicht als sachgerecht empfunden.

Kriminalistische „Hypothesen“ sind auf Tatsachen begründete, in der Regel variantenhafte bzw. alternative Erklärungsmodelle für kriminalistisch relevante Sachverhalte. Mit Hilfe der Hypothesen wird versucht, die zeitliche und sachliche Abfolge des noch ungeordnet erscheinenden Geschehens darzustellen (im Unterschied zur wissenschaftlichen Hypothese). Die von Behörden verwendete Software dient nicht zur Erstellung von Hypothesen oder gar zur automatisierten Strafverfolgung, sondern zur Überprüfung von Hypothesen und zur Unterstützung der Strafverfolgung. Es sind nicht Computer, welche Zusammenhänge zwischen Personen, Sachen und Orten analysieren, sondern die Sachbearbeiter werden durch Software bei dieser Tätigkeit unterstützt.

Mit den Fragen 19 und 20 werden Auskünfte zu Sachverhalten begehrt, die aufgrund der Folgen, die bei ihrer Veröffentlichung zu erwarten sind, zum Teil als „geheimzuhaltende Tatsache“ im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) i. V. m. der Verschlusssachenanweisung (VSA) eingestuft wurden. Die Kenntnisnahme von Einzelheiten zu den technischen Fähigkeiten der Bundesbehörden könnte sich nach der Veröffentlichung der Antworten der Bundesregierung auf diese Fragen nachteilig für die Interessen der Bundesrepublik Deutschland auswirken. Aus ihrem Bekanntwerden könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf die Arbeitsweisen und die Fähigkeiten der Behörden des Bundes ziehen. Im Ergebnis würde dadurch die Funktionsfähigkeit der Sicherheitsbehörden und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt bzw. gefährdet. Diese Informationen wurden daher gemäß § 3 Nummer 2 VSA als „Geheim“ eingestuft. Die Antworten zu diesen Fragen wurden mit der Einstufung „Geheim“ dem Deutschen Bundestag übermittelt.

1. Teilt die Bundesregierung die Ansicht der EU-Innenkommissarin Cecilia Malmström, dass es sich bei den im Kommissionsdokument E-000171/2012 beschriebenen Werkzeugen bzw. Vorgängen um ein „Data Mining“ durch die EU-Polizeiagentur Europol handelt?

Eine Beurteilung, ob die im Bezugsdokument E-000171/2012 genannten Werkzeuge und Vorgänge die Eigenschaften eines „Data Mining“-Verfahrens erfüllen, ist nicht möglich, da das Bezugsdokument nicht in ausreichender Tiefe auf deren Methodik und Algorithmen eingeht. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

- a) Sofern es sich aus Sicht der Bundesregierung nicht um „Data Mining“ handelt, wie würde sie die beschriebene Nutzung „akademische[r] Software“ und eines „speziellen Analyserahmen[s]“ ansonsten klassifizieren, der demnach zum Einsatz kommt, um „Netzkomponenten, Subnetze und Schnittpunkte zu analysieren, Zentralität zu ermitteln und die wichtigsten Akteure herauszufiltern“?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

- b) Inwiefern sind Bundesbehörden über den Einsatz von Software der Firmen i2 und Themis bzw. des „Freeware-Tools (Pajek)“ bei Europol informiert?

Nach Kenntnis der Bundesregierung setzt Europol im Rahmen von Analyse-Workflows Produkte der Firmen IBM (ehemals i2 Group) und Themis sowie die Freeware Pajek ein.

- c) Inwiefern haben auch Bundesbehörden bereits von Software der Firmen i2 und Themis mittelbar oder unmittelbar bei Europol Gebrauch gemacht?

Die von Europol eingesetzten Softwareprodukte der Firmen i2 und Themis stehen den Beschäftigten von Europol zur Verfügung. Nach Artikel 14 Absatz 2 des Beschlusses 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) wird für jedes Analyseprojekt eine Analysegruppe gebildet, an der auch Verbindungsbeamte und/oder Experten der Mitgliedstaaten, von denen die Informationen stammen, teilnehmen. Diese Verbindungsbeamten und/oder Experten können zwar keine Daten in das Analyse-system eingeben oder Daten im Analysesystem ändern, aber sie können Daten abrufen. Insoweit können auch die Verbindungsbeamten und/oder Experten der Mitgliedstaaten die bei Europol eingesetzte Software nutzen.

2. Welche datenschutzrechtlichen Vorgaben gelten für Europol bei der Analyse von Netzkomponenten, Subnetze[n] und Schnittpunkte[n]?

Inwiefern ist nach Ansicht der Bundesregierung hiervon auch ein „Data Mining“ erfasst?

Die für Europol geltenden datenschutzrechtlichen Vorgaben ergeben sich primär aus dem Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol). Mit Blick auf die dort verfügbaren Analyse-Workflows ist insbesondere auf die Artikel 14 und 16 sowie auf die gemeinsamen Bestimmungen zur Informationsverarbeitung (Artikel 17 bis 21) und die Bestimmungen zum Datenschutz und zur Datensicherheit (Artikel 27 bis 35) hinzuweisen. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

3. Inwieweit nutzt die FRONTEX Verfahren zur automatisierten Analyse von Personen- oder Sachdaten?

Nach Kenntnis der Bundesregierung nutzt die EU Grenzschutzagentur FRONTEX automatisierte Anwendungen für die Auswertung von offenen Quellen und Medienberichterstattung im Internet. Dabei handelt es sich um webbasierte Anwendungen, die der Sammlung und Darstellung von Informationen in der Weltpresse dienen.

- a) Inwieweit trifft es zu, dass FRONTEX für das „Common Pre-frontier Intelligence Picture“ an Verfahren zum „Text Mining“ forscht?

Es gibt derzeit Überlegungen, Anwendungen zur automatisierten Datenauswertung für das „Common Pre-Frontier Intelligence Picture“ (CPIP) als Bestandteil des europäischen Grenzüberwachungssystems EUROSUR nutzbar zu machen. Bisher gibt es keine entsprechende betriebsbereite Anwendung.

- b) Worin besteht die Aufgabe der FRONTEX innerhalb des Forschungsprojekts OPTIMA?

Der Bundesregierung ist nicht bekannt, ob und inwieweit die Agentur an einem Forschungsprojekt „OPTIMA“ beteiligt ist.

4. Teilt die Bundesregierung die Ansicht der Fragesteller, dass es sich beim „Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, d[em] Ausschluss von unbedeutenden Informationen und Erkenntnissen, d[er] Zuordnung eingehender Informationen zu erkannten Sachverhalten sowie d[er] statistische[n] Auswertung der gespeicherten Daten“ um „Data Mining“ handelt?

Falls nein, worin läge eine andere Definition von „Data Mining“ bzw. der beschriebenen Vorgänge?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. Welche datenschutzrechtlichen Vorgaben gelten im Zuständigkeitsbereich des BMI bei einem „Data Mining“ bzw. der Verknüpfung von im Internet oder anderen öffentlichen Quellen ermittelten Informationen mit anderen Datensätzen für Behörden des Bundes (Bundestagsdrucksache 17/6587)?

Es gelten die datenschutzrechtlichen Vorgaben, die sich aus dem Bundesdatenschutzgesetz (BDSG), der Strafprozessordnung (StPO) und den jeweiligen Fachgesetzen ergeben.

- a) Welche weitergehenden Arbeitsanweisungen existieren bei welchen Behörden?

Bei den Polizeien des Bundes und dem Bundesamt für Verfassungsschutz (BfV) sind weitergehende datenschutzrechtliche Arbeitsanweisungen in der Regel in Datei- und Errichtungsanordnungen sowie Dienstanweisungen entsprechend den einschlägigen rechtlichen Vorgaben enthalten. Insbesondere bei Datei- und Errichtungsanordnungen besteht regelmäßig eine Beteiligungspflicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

- b) Inwieweit sehen Errichtungsanordnungen für andere vom BKA geführte Datensammlungen bereits eine „erweiterte Nutzung“ im Sinne der Fragestellung vor?

In den Errichtungsanordnungen sind unter anderem die Rechtsgrundlage und der Zweck der jeweiligen Datei festzulegen (vgl. etwa § 490 StPO). Für welche Zwecke die Dateien genutzt werden dürfen, ergibt sich aus den gesetzlichen Bestimmungen. So dürfen beispielsweise nach § 98c StPO personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden, ohne dass dies in einer Errichtungsanordnung nochmals explizite Erwähnung finden muss.

- c) Inwieweit stimmt die Bundesregierung der Ansicht der Fragesteller zu, dass für eine „Gewichtung“ von Suchkriterien oder einer Suche nach „unstrukturierten Informationen“ in anderen vom BKA geführten Datensammlungen eine neue Errichtungsanordnung erforderlich wäre?

Die Frage lässt sich nicht allgemein beantworten. So entbindet etwa § 490 Satz 2 StPO von dem Erfordernis einer Errichtungsanordnung für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

6. Inwieweit nutzen Behörden des BMI „Werkzeuge zur Detailanalyse und Visualisierung von Beziehungen zwischen physischen Merkmalen und allen dazu verfügbaren Informationen“, wie sie die Firma i2 auf dem Europäischen Polizeikongress bewarb?

Verschiedene der von Sicherheitsbehörden genutzten Anwendungen, u. a. Analyst's Notebook, sind in der Lage, räumliche und sonstige Beziehungen (Täter, Mittäter, Fahrer, Beifahrer etc.) zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darzustellen.

- a) Seit wann kommt das von der Firma vertriebene „Analyst's Notebook“ bei Behörden des BMI zum Einsatz?

Analyst's Notebook wird vom Bundeskriminalamt (BKA) ca. seit dem Jahr 2000, von der Bundespolizei ca. seit dem Jahr 2002 und vom BfV ca. seit dem Jahr 1994 genutzt.

- b) Welche Kosten für Beschaffung, Wartung und Lizenzen fielen seitdem an?

Im BKA sind Gesamtkosten in der Höhe von 389 749,67 Euro (seit 2002), bei der Bundespolizei in der Höhe von ca. 245 000 Euro (seit 2008) und beim BfV in der Höhe von 240 000 Euro angefallen.

- c) Von wem wurde die Software konkret beschafft?

Das Produkt Analyst's Notebook der Firma i2 wurde von den jeweiligen Behörden über die Firma rola Security Solutions GmbH beschafft. Diese war bis Ende 2010 alleiniger Vertriebspartner von i2-Produkten in Deutschland.

- d) Inwieweit werden auch die Anwendungen „Social Network Analysis“, „Quick-Navigator“, „Google Earth-Plug-in“ sowie weitere „Filter und Histogramme“ eingebunden?

Die genannten Funktionen gehören zwar zum Standardlieferumfang von Analyst's Notebook und sind daher in die Software eingebunden, sie werden von den Behörden jedoch nur teilweise genutzt.

7. Auf welche beim BKA geführte Datensammlungen darf „Analyst's Notebook“ zugreifen?

Eine generelle Zugriffsmöglichkeit von Analyst's Notebook auf beim BKA geführte Datensammlungen besteht nicht. Im BKA steht eine Schnittstelle zwischen dem Fallbearbeitungssystem b-case und Analyst's Notebook zur Verfügung, mit deren Hilfe Daten im Einzelfall zur Nutzung in Analyst's Notebook exportiert werden können.

- a) Welche Art von „Hypothesen“ gibt „Analyst's Notebook“ aus, und wie werden diese im Regelfall weiter prozessiert?

Bei Analyst's Notebook handelt es sich primär um eine Software zur Visualisierung von Beziehungsgeflechten. Die Visualisierungskomponente wird durch spezielle Analysefunktionalitäten unterstützt. Als Visualisierungs- und Analysetool kann Analyst's Notebook eigenständig keine Hypothesen erstellen, sondern nur die polizeiliche Sachbearbeitung bei der Beantwortung bestimmter Fragestellungen unterstützen. Auf Basis der Ergebnisse von Analyst's Notebook können durch den/die polizeilichen Sachbearbeiter/innen Hypothesen erstellt und ggf. verifiziert bzw. falsifiziert werden.

- b) Hat die Nutzung von „Analyst's Notebook“ nach Ansicht der Bundesregierung dazu beigetragen, die Strafverfolgung oder Gefahrenabwehr bei Bundesbehörden zu erleichtern?

Die Polizeien des Bundes berichteten dazu, dass Analyst's Notebook eine geeignete Software sei, um Beziehungsgeflechte und Verbindungen zwischen Objekten zu visualisieren und zu analysieren. In diesem Rahmen unterstütze der Einsatz von Analyst's Notebook die Strafverfolgung und grundsätzlich auch die Gefahrenabwehr.

8. Auf welche Art und Weise unterstützt die Inhaltliche Datenträgerauswertung (IDA) des BKA auch eine „Auswertung von Texten“ (Antwort auf die Schriftliche Frage 19 auf Bundestagsdrucksache 17/10925)?

Die Inhaltliche Datenträgerauswertung (IDA) unterstützt die Auswertung von Texten in der Form, dass IDA einen Volltextindex, basierend auf den vorhandenen Dateien erstellt. Dieser ist durchsuchbar; Recherchetreffer werden optisch hervorgehoben dargestellt.

- a) Auf welche Art und Weise und nach welchem mathematischen Verfahren werden Dateien „bewertet“?

Die Bewertung der in IDA vorliegenden Dateien erfolgt nicht nach einem „mathematischen Verfahren“, sondern im Rahmen der polizeifachlichen Sachbearbeitung.

- b) Was ist gemeint, wenn die Bundesregierung diesbezüglich von einer „Erkennung unterschiedlicher Sprachen“ schreibt?

In IDA vorliegende Texte können im Hinblick auf die genutzte Sprache identifiziert werden. Die Erkennung der Landessprache basiert auf einer Worterkennung in Verbindung mit entsprechenden Wörterbüchern.

- c) In welchem Umfang wurde die IDA bereits in der „Zusammenfassung mehrerer Ermittlungsverfahren“ eingesetzt?

IDA wurde bisher nicht für die Zusammenfassung mehrerer Ermittlungsverfahren eingesetzt.

- d) Da die Bundesregierung die Auffassung vertritt, die IDA sei keine rasternde Analysesoftware, auf welche Weise nehmen Bundesbehörden dann derartige Ermittlungen vor?

Der Begriff „Rasterung“ wird im juristischen Sprachgebrauch nur im Zusammenhang mit der Rasterfahndung gemäß den §§ 98a, 98b StPO und § 20j des Bundeskriminalamtgesetzes (BKAG) verwendet. Hierzu wird auf die Antwort zu Frage 13 verwiesen.

9. Inwiefern hat die Nutzung von Werkzeugen wie „Analyst’s Notebook“ oder „Infozoom“ der Firma humanIT Software GmbH bei Polizeien des Bundes in den letzten fünf Jahren zugenommen (Bundestagsdrucksache 17/8089)?

In welchem Umfang werden „Analyst’s Notebook“ und „Infozoom“ auch zur Gefahrenabwehr eingesetzt?

Beim BKA hat die Nutzung von Analyst’s Notebook und Infozoom geringfügig zugenommen. In Einzelfällen werden Analyst’s Notebook und Infozoom durch das BKA auch zur Gefahrenabwehr eingesetzt.

Bei der Bundespolizei erfolgt die Nutzung von Analyst’s Notebook und Infozoom auf gleichbleibendem Niveau. Die Bundespolizei nutzt Analyst’s Notebook nicht im Rahmen der Gefahrenabwehr. Infozoom dient ausschließlich zur Auswertung der Polizeilichen Kriminalstatistik (PKS).

Die Anzahl paralleler behördlicher Nutzer von Analyst’s Notebook im Zollfahndungsdienst (ZFD) ist weitgehend gleichgeblieben. Weitergehende Aufzeichnungen werden nicht geführt. In geeigneten Fällen wird Analyst’s Notebook durch den ZFD auch zur zollrechtlichen Gefahrenabwehr eingesetzt. Infozoom wird durch den ZFD nicht genutzt.

10. Mit welchen Verfahren sollen die in der „Rechtsextremismusdatei“ gesammelten Daten einer „erweiterten Nutzung“ unterzogen werden?

Mit welchen Verfahren die in der „Rechtsextremismusdatei“ (RED) gespeicherten Daten einer „erweiterten Nutzung“ unterzogen werden, ist zurzeit noch nicht abschließend festgelegt.

- a) Welche „Projektphasen“ existieren für den Aufbau der Datensammlung, wie es die Bundesregierung in der Fragestunde des Deutschen Bundestages am 26. September 2012 berichtet?

Für die Errichtung der RED sind drei Projektphasen vorgesehen. Die erste Projektphase umfasst die Bereitstellung der Grundfunktionalitäten der RED, die zweite und dritte Projektphase dienen der Umsetzung der „erweiterten Nutzung“.

- b) Welche Schritte enthält die entsprechende „Projektphase“ zur „erweiterten Nutzung“?

Eine detaillierte Projektplanung für die Projektphasen zwei und drei liegt zurzeit noch nicht vor.

- c) Wer ist an der Definition, Entwicklung und Beschaffung der notwendigen technischen sowie sonstigen Mittel beteiligt?

Die Definition technischer Anforderungen und Mittel erfolgt durch die an der RED beteiligten Bundes- und Landesbehörden. Die Entwicklung und Beschaffung obliegt dem BKA.

- d) Über welche Funktionalitäten verfügt die „Anwendungssoftware“, mit der das BKA bereits jetzt Daten in der „Rechtsextremismusdatei“ verarbeitet?

Die Softwareanwendung RED kann im Rahmen der Datenverarbeitung Datensätze zu Personen, Organisationen und Sachen nach § 2 des Rechtsextremismus-Datei-Gesetzes (RED-G) mit den Datenarten nach § 3 RED-G anlegen, ändern und löschen. Nach § 4 RED-G kann die Speicherung auch beschränkt oder verdeckt erfolgen. Diese Funktionalitäten können sowohl über eine Eingabemaske als auch über eine Schnittstelle zur Befüllung, Aktualisierung und Löschung von Datensätzen in teilautomatischen Schritten genutzt werden. Darüber hinaus können nach § 12 Absatz 3 RED-G Daten gesperrt werden. Die Daten der RED können bei Vorliegen einer entsprechenden Berechtigung gemäß § 5 RED-G abgefragt werden.

- e) Inwiefern dient „Inpol-Fall“ wie im Falle der „Antiterrordatei“ auch bei der „Rechtsextremismusdatei“ als „Quellsystem“ (Bundestagsdrucksache 17/8544 – neu)?

„INPOL-Fall“ ist eines der Quellsysteme für die Rechtsextremismusdatei.

11. Inwieweit ist eine „erweiterte Nutzung“ auch für andere polizeiliche oder geheimdienstliche Datensammlungen beabsichtigt?

Der Begriff „erweiterte Nutzung“ wurde in § 7 RED-G spezifisch für die RED geregelt, um eine beschränkte Nutzung der in der Datei enthaltenen Daten über die Indexfunktion hinaus zu eröffnen. Im Übrigen findet eine „erweiterte Nutzung“ nach Maßgabe der gesetzlichen Bestimmungen bereits heute in der polizeilichen wie auch der nachrichtendienstlichen Praxis statt (vgl. die Antwort zu Frage 12).

12. Mit welchen technischen Mitteln sind Behörden der Bundesregierung bereits in der Lage, wie für die „Rechtsextremismusdatei“ geplant, „räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen“ darzustellen sowie „die Suchkriterien [zu] gewichten“?

Räumliche und sonstige Beziehungen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen können in verschiedenen Datenbanken und Softwareprodukten abgebildet werden. Hierzu zählen unter anderem INPOL-Fall, b-case und Analyst's Notebook.

- a) Wie gestalten Behörden die Suche nach phonetischen oder unvollständigen Daten, bzw. welche Kapazitäten werden hierfür entwickelt?

Die Suche nach phonetischen oder unvollständigen Daten ist in verschiedenen Datenbankanwendungen über hinterlegte Logiken möglich. Spezielle Kapazitäten werden hierfür nicht entwickelt.

- b) Wie gestalten Behörden die Suche über eine Mehrzahl von Datenfeldern, bzw. welche Kapazitäten werden hierfür entwickelt?

Die Suche über eine Kombination von Datenfeldern ist in verschiedenen Datenbankanwendungen möglich. Hierbei können beispielsweise bei einer Suche mehrere Datenfelder eines Objektes mit Suchbegriffen belegt werden. Spezielle Kapazitäten werden hierfür nicht entwickelt.

- c) Wie gestalten Behörden die Verknüpfung von Personen, Institutionen, Organisationen, Sachen, bzw. welche Kapazitäten werden hierfür entwickelt?

Die Verknüpfung von Personen, Institutionen, Organisationen und Sachen ist in verschiedenen Datenbankanwendungen möglich. Hierbei werden zwei oder mehr Objekte eines Datenbestands über Beziehungsobjekte miteinander verknüpft. Spezielle Kapazitäten werden hierfür nicht entwickelt.

- d) Wie gestalten Behörden die zeitliche Eingrenzung der Suchkriterien, bzw. welche Kapazitäten werden hierfür entwickelt?

Die Fachobjekte und Beziehungen von verschiedenen Datenbankanwendungen enthalten Datumsinformationen. Diese Datumsinformationen können bei Suchen berücksichtigt werden. Spezielle Kapazitäten werden hierfür nicht entwickelt.

- e) Sofern die Bundesregierung zur in den Fragen 12a bis 12d beschriebenen Suche noch nicht in der Lage ist, auf welche Art und Weise wird die entsprechende technische Umsetzung betrieben, bzw. welche Kapazitäten werden hierfür entwickelt?

Auf die Antworten zu den Fragen 12a bis 12d wird verwiesen.

13. Welche Software mit welchen Zusatzfunktionen wird bei Bundesbehörden normalerweise für eine Rasterfahndung eingesetzt?

Rasterfahndungen gestalten sich je nach Ausgangslage vollkommen unterschiedlich. Es existiert daher keine Standardsoftware für „die“ Rasterfahndung.

- a) Welche Definition existiert bei Bundesbehörden für den Begriff „Rasterfahndung“, und wie wird diese zu „Data Mining“ abgegrenzt?

Eine Rasterfahndung umfasst die maschinell ablaufende Suche in Datenbeständen öffentlicher und nichtöffentlicher Stellen nach auf den Täter vermutlich zutreffenden Prüfungsmerkmalen. Die Rasterfahndung aus repressiven Gründen richtet sich nach den Bestimmungen der §§ 98a, 98b StPO. Die Rasterfahndung aus präventiven Gründen richtet sich nach den jeweiligen Bestimmungen der Länder bzw. nach § 20j des Bundeskriminalamtgesetzes (BKAG). Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

- b) Inwieweit wurden die Massendaten im Zusammenhang mit der (damals noch nicht bekannten) Täterschaft des NSU auch mit „Rasterfahndungen“ prozessiert?

Eine Rasterfahndung wurde durch das BKA im Rahmen des NSU-Ermittlungskomplexes nicht durchgeführt. Im Übrigen wird auf die Antwort auf die Schriftliche Frage 9 auf Bundestagsdrucksache 17/11283 des Abgeordneten Andrej Hunko vom 23. Oktober 2012 verwiesen.

- c) Wie viele Anordnungen zur Rasterfahndung sind nach Kenntnis der Bundesregierung von Gerichten ergangen, und wie viele Ersuchen wurden zurückgewiesen?

Im BKA wurde in den vergangenen fünf Jahren eine Rasterfahndung durchgeführt. Dabei wurde durch die zuständige Staatsanwaltschaft eine Rasterfahndung wegen schweren sexuellen Missbrauchs eines Kindes beantragt. Vom zuständigen Gericht wurde der durch die Staatsanwaltschaft beantragte Beschluss erlassen. Über Rasterfahndungen der Bundesländer hat die Bundesregierung keine Übersicht.

- d) In welchen weiteren Datenbeständen durfte nach Erlass der Beschlüsse jeweils gesucht werden?

Die in der Antwort zu Frage 13c genannte Rasterfahndung bezog sich auf Informationen aus dem Melderegister und dem standesamtlichen Geburtsregister.

14. Mit welcher Software mit welchen Funktionalitäten und welchen Zusatzfunktionen werden bei Bundesbehörden „Massendaten“ verarbeitet?

Der Begriff der Massendaten im Sinne einer umfangreichen Datenmenge ist dem Alltagssprachgebrauch entsprungen. Für die Arbeit von Bundesbehörden stellt er keine relevante Kategorie dar, die im Rahmen der Anwendung gesetzlicher Befugnisse eine Rolle spielt. Auf den Hinweis in der Vorbemerkung wird verwiesen.

Massendaten im vorgenannten Sinne werden durch das BKA in den polizeilichen Fallbearbeitungssystemen, b-case und INPOL, sowie in folgenden speziellen Auswertungsanwendungen bearbeitet:

- IDA zur Auswertung elektronischer Datenträger im Ermittlungsverfahren,
- Die Software „Hermes“ der Firma SYBORG zur Bearbeitung und Auswertung von Telekommunikationsüberwachungen,
- INFOZOOM der Firma Human IT zur Filterung von Daten in Tabellenform,
- Analyst's Notebook zur grafischen Darstellung von Daten aus Listen und Datenbanken,

- EXCEL zur Erstellung von Filtern und Sortierung von Daten in Tabellenform,
- MySQL zur Datenaufbereitung.

Durch die Bundespolizei werden „Massendaten“ mit den Anwendungen b-case und Analyst's Notebook bearbeitet.

In der Zollverwaltung werden anfallende tabellarische Massendaten mit der Software Analyst's Notebook analysiert. Zusatzfunktionen bzw. kompatible andere Produkte des Herstellers sind nicht im Einsatz. Ferner erfolgt eine Bearbeitung von Massendaten im vorgenannten Sinne im Zollfahndungsinformationssystem INZOLL und, sofern es der Umfang der zu analysierenden Datenmengen und die konkrete Fragestellung zulassen, auch über Excel. Sofern Standardprodukte nicht ausreichen, um das Ziel des Reduzierens von Massendaten auf die relevante Anzahl zu erreichen, werden darüber hinaus im ZFD einzel-fallbezogen eigene, auf Basis der Datenbank Oracle entwickelte Programme eingesetzt. Gründe für solche Eigenentwicklungen bestehen in der Regel darin, dass bestimmte Datenformate von Standardprodukten nicht verarbeitet werden können oder aber die mathematischen Plausibilitäten bzw. Algorithmen der Standardprodukte zu grob sind, um relevante Feintreffer zu filtern (z. B. steuerlich relevante Berechnungsmethoden). Für die Erschließung großer Datenmengen, die sowohl papiermäßig als auch digital vorliegen können, wird das System ZyLAB verwendet.

Mit ZyLAB können Papierdokumente digitalisiert, digitalisierte und bereits digital vorhandene Dokumente indiziert und gespeichert werden. Mit Hilfe der indizierten Begriffe ist es möglich, in umfangreichen Datenbeständen durch Suchen nach Begriffen oder Begriffskombinationen relevante Dokumente schnell wieder aufzufinden und die Datenbestände dadurch zeitnah zu erschließen.

Zur Bearbeitung und Auswertung von Telekommunikationsüberwachungen wird durch den ZFD die Software der Firma DigiTask eingesetzt.

Für die ermittlungsfallbezogene Auswertung beschlagnahmter Datenträger wird in der Zollverwaltung hauptsächlich die Software X-Ways eingesetzt. Spezielle Auswerteanwendungen (wie z. B. IDA) stehen darüber hinaus nicht zur Verfügung.

Beim Bundesnachrichtendienst (BND) werden Massendaten im vorgenannten Sinne mit Hilfe einer Software aufbereitet, die durch eine externe Firma speziell für den Bundesnachrichtendienst entwickelt wurde. Die so aufbereiteten Daten werden mittels MS Excel weiterverarbeitet und mit der Software Analyst's Notebook visualisiert.

Beim BfV wird innerhalb des Nachrichtendienstlichen Informationssystems „NADIS WN“ mit dem Verfahren „VAMP“ (Verfahren zur Abwicklung von Massendaten und Prozesssteuerung) der behördliche Datenaustausch organisiert, vor allem im Rahmen der Wahrnehmung der gesetzlichen Aufgaben. Durch das BfV werden jedoch keine Massendatenverfahren angewendet, bei denen eine große Menge von Ausgangsdaten abgerufen wird, unter der die für Aufgabenerfüllung des BfV wertigen Elemente nur als kleine Teilmengen zu vermuten ist.

- a) Welche Löschfristen existieren für die verschiedenen „Massendaten“ jeweils im Regelfall und im hier behandelten Fall?

Für das BKA richten sich die Löschfristen nach den einschlägigen gesetzlichen Vorgaben zur Speicherung von Daten im Rahmen der Zentralstellen- oder Strafverfolgungsaufgaben des BKA. Für Zwecke eines Strafverfahrens nach den

§§ 483 ff. StPO gespeicherte Daten sind nach näherer Maßgabe des § 489 StPO grundsätzlich dann zu löschen, wenn ihre Speicherung unzulässig ist oder sich aus Anlass einer Einzelfallbearbeitung ergibt, dass die Kenntnis der Daten für die in den §§ 483, 484, 485 StPO jeweils bezeichneten Zwecke nicht mehr erforderlich ist. Für die Rasterfahndung nach § 98a StPO enthalten § 98b Absatz 3 Satz 2 und § 101 Absatz 8 StPO zudem spezielle Löschungsbestimmungen. Im Übrigen richtet sich die Löschung insbesondere nach § 32 BKAG.

Für die Bundespolizei gelten hinsichtlich der Löschfristen die einschlägigen Vorschriften des Bundespolizeigesetzes (BPolG), der StPO und des BDSG.

Für die Zollverwaltung richten sich die Löschfristen nach den gesetzlichen Vorgaben des Zollfahndungsdienstgesetzes (ZFdG), der StPO und, soweit darüber hinaus einschlägig, nach Vorgaben des BDSG.

Für den BND richten sich die Löschfristen nach den gesetzlichen Vorgaben des BND-Gesetzes (BNDG) i. V. m. mit dem Bundesverfassungsschutzgesetz (BVerfSchG) und des BDSG.

Für das BfV richten sich die Löschfristen nach den gesetzlichen Vorgaben des BVerfSchG und des BDSG.

- b) Wie viele sogenannte Massendaten wurden bzw. werden in den Ermittlungen wegen der ungeklärten Mordfälle bis zur Entdeckung der Täterschaft des „Nationalsozialistischen Untergrunds“ von den damit befassten Bundes- und Landesbehörden nach Kenntnis der Bundesregierung erhoben, gespeichert oder verarbeitet?

Im Zusammenhang mit den Taten des Nationalsozialistischen Untergrunds wurden Daten aus insgesamt 27 Ermittlungsverfahren, die sich über einen Zeitraum von mehr als 10 Jahren erstrecken, beim BKA zusammengeführt.

Bei den 27 Tathandlungen handelt es sich um

- 10 Tötungsdelikte (9 Ceska-Komplex, 1 Heilbronn),
- 2 versuchte Tötungsdelikte [Sprengstoffanschläge in Köln, Lebensmittelgeschäft 1 Verletzte; Keupstraße, 22 Verletzte] sowie
- 15 Raubdelikte.

Insgesamt wurden 20 575 657 Funkzellendatensätze (gemäß § 100g Absatz 2 Satz 2 StPO) und 13 842 Datensätze zu Anschlussinhabern (gemäß § 113 TKG) vornehmlich aus den bei bereits bei den Landespolizeibehörden gespeicherten Daten zusammengeführt. Eine geringe Anzahl von Funkzellendatensätzen bzw. Bestandsdaten wurde im Zusammenhang mit den Tatorten Eisenach und Chemnitz zusätzlich durch das BKA erhoben.

Informationen zu Finanztransaktionen, Hotelbuchungen und Mietwagennutzungen sind das Ergebnis gezielter Ermittlungen. Sie sind somit auch nicht von dem sog. Massendatenabgleich, bei dem die unterschiedlichen polizeilichen Systeme nach übereinstimmenden Datenbeständen überprüft werden, umfasst.

- c) Welche Software kam hier nach Kenntnis der Bundesregierung mit welchen Funktionalitäten zum Einsatz?

Die Verarbeitung von großen Datenmengen, die in elektronischer Form erhoben wurden, erfolgt mit den in der Antwort zu Frage 14 genannten Tools, die auch bei der EG ST TRIO (ehemals BAO ST TRIO) eingesetzt wurden.

15. Welche „verbundrelevante[n] Daten oder im Zusammenhang mit Großschadenslagen gewonnene[n] Daten“ werden derzeit automatisiert an „Inpol-Fall“ übertragen?

Eine automatisierte Übertragung von Daten an INPOL-Fall-Verbundanwendungen findet nicht statt. Der Übertragung von Daten über Bund-Länder-Datei-Schnittstellen (BLDS) geht eine Einzeldatensatzprüfung durch einen Sachbearbeiter in den Quellenwendungen voraus. Eine Ausnahme bildet hier die Anlieferung von Daten an die INPOL-Fall-Anwendungen „Streugut“ und „Lagefall BAO“, welche automatisiert beliefert werden können.

- a) Wann und von wem wurden die Bund-Länder-Datei-Schnittstelle (BLDS) und die Bund-Länder-Online-Schnittstelle (BLOS) im BKA entwickelt?

Die BLDS wurde 2006 im Rahmen der Vorbereitung auf die Fußballweltmeisterschaft 2006 in Deutschland und das in diesem Zusammenhang durchzuführende Akkreditierungsverfahren durch das BKA und dessen damaligen externen Dienstleister entwickelt. Die Bund-Länder-Online-Schnittstelle (BLOS) wurde ebenfalls im BKA entwickelt und steht seit Ende des Jahres 2007 zur Verfügung.

- b) Inwiefern trifft es zu, dass die BDLS bzw. die BLOS im Auftrag der damals erfolglos ermittelnden Besondere Aufbauorganisation Bosporus eingerichtet wurde?

Die Aussage trifft nicht zu.

- c) Welche Kosten sind hierfür entstanden, und wer hat diese getragen?

Bei der BLDS bzw. der BLOS handelt es sich um Eigenentwicklungen des BKA. Hierbei wurden neben internen Entwicklern auch externe Entwickler beschäftigt, die über den damaligen Rahmenvertrag auch in anderen Projekten eingesetzt waren. Eine belastbare, detaillierte Erhebung des Anteils externer Entwicklungsleistung, explizit für die BLDS bzw. BLOS, ist nicht möglich.

- d) Inwiefern kann die Bundesregierung die Lieferung der BDLS bzw. BLOS durch die Firma rola security solutions GmbH als erfolgreich bewerten?

Bei der von INPOL-Fall angebotenen BLDS und BLOS handelt es sich um Eigenentwicklungen des BKA. Die rsCase-Schnittstellenmodule BLDS und BLOS wurden im Fallbearbeitungssystem b-case der Firma rola implementiert, getestet und fachlich freigegeben. Die Schnittstellenmodule sind produktiv im Einsatz. Mit der Freigabe dieser Schnittstellenmodule kann die Lieferung der Anpassung an die BLDS und die BLOS durch die Firma rola als erfolgreich bewertet werden.

- e) Sofern die Bundesregierung Nachbesserungsbedarf sieht, wo läge dieser?

Bei der von INPOL-Fall angebotenen BLDS handelt es sich um eine Eigenentwicklung des BKA. Ein Nachbesserungsbedarf bei der von INPOL-Fall angebotenen BLDS durch die Firma rola besteht daher nicht. Die rsCase-Schnittstellenmodule BLDS und BLOS im Fallbearbeitungssystem b-case wurden gemäß dem mit der Firma Rola abgestimmten Konzept umgesetzt. An den rsCase-Schnittstellenmodulen BLDS und BLOS besteht aktuell kein Nachbesserungsbedarf.

- f) Worin besteht die „Weiterentwicklung“ von „Inpol-Fall“, die „auf Basis der Landesfallsoftware ‚Crime‘“ aus Hamburg und Hessen „durch das BKA selbst“ vorgenommen wurde?

Schwerpunkt der Weiterentwicklung waren besondere Anforderungen an Verbunddateien, die im System INPOL-Fall betrieben werden.

16. Auf welche Art und Weise und mit welchen Funktionalitäten wurde die Analysesoftware des BKA „B-case“ der Firma rola Security Solutions GmbH „BKA-spezifisch angepasst“ (Bundestagsdrucksache 17/8544 – neu)?

Welche „grundsätzlich alle beschafften Module“ sind in der vom BKA beschafften Analysesoftware „B-case“ eingebunden?

Für das Fallbearbeitungssystem b-case des BKA wurden und werden folgende BKA-spezifische Anpassungen des Produktes rsCase vorgenommen bzw. werden folgende auf einer spezifischen BKA-Anforderung basierende Module eingebunden:

- Schnittstelle zwischen b-case und dem Vorgangsbearbeitungssystem des BKA „VBS“;
- Schnittstelle zwischen b-case und der SSO (Single Sign On) des BKA,
- Modul: Wiedervorlage Bund,
- Modul: Erweiterte Verfahrenssichten,
- Anbindung an den zentralen Protokollserver des BKA,
- Anbindung von b-case an die Diensteüberwachung des BKA,
- Anpassung der Namens und Straßensuche in b-case gemäß BKA-Vorgaben,
- Anpassungen der Schnittstellenkonfiguration- und Administration gemäß BKA-Vorgaben,
- Ertüchtigung von b-case für MapViewer WMS-getMap Request.

Zur Übernahme von TKÜ-Daten aus der TKÜ-Anlage wurde eine weitere Schnittstelle geschaffen. Prinzipiell können alle von der Firma rola im Rahmen des Produkts rsCase angebotenen Schnittstellen und Module in rsCase eingebunden werden.

17. In wie vielen Fällen wurden in den letzten fünf Jahren „auf Antrag der ermittlungsführenden Abteilung“ über eine Schnittstelle Daten aus der Telekommunikationsüberwachung (TKÜ-Daten) an „rsCase“ bzw. „B-case“ von Bundespolizei und BKA übertragen (bitte als Tabelle aufschlüsseln)?

Ausleitungen von TKÜ-Daten an die Fallbearbeitungssysteme werden durch das BKA nicht statistisch erfasst.

Bei der Bundespolizei erfolgt die Datenerhebung in Ermittlungsverfahren auf Grundlage einer datenschutzrechtlichen Errichtungsanordnung gemäß § 36 BPolG.

Aus der TKÜ wurden Erkenntnisse von den zu überwachenden Anschlüssen (ZÜA) an das Fallbearbeitungssystem b-case wie folgt übertragen:

2009 (1. Juli bis 31. Dezember)	aus 25 ZÜA
2010	aus 281 ZÜA
2011	aus 491 ZÜA
2012 (1. Januar bis 30. September)	aus 290 ZÜA.

18. Wie ist es gemeint, wenn die Bundesregierung erklärt, eine Suche von unstrukturierten Datenbeständen der Bundespolizei sowie in „B-case“ und „Inpol-Fall“ könne „nur mittels Volltextrecherche“ erfolgen?

Mit Volltextrecherche wird die Suche nach einem oder mehreren Worten in einem Datensatz oder Dokument beschrieben. Im Fallbearbeitungssystem b-case und in INPOL-Fall werden hierfür die in den Datenbanken generell implementierten Funktionalitäten genutzt.

19. Inwieweit haben Behörden des BMI im Jahr 2012 „prediktive Software“ oder Software zum „Data Mining“ getestet oder Testberichte anderer deutscher Stellen hierzu erhalten?

Im Jahr 2012 wurde durch das BKA, die Bundespolizei und das Bundesamt für Sicherheit in der Informationstechnik weder prediktive Software noch Software zum „Data Mining“ nach der Definition der Fragesteller getestet. Hierzu erhielten diese Stellen auch keine Testberichte anderer deutscher Stellen. Gleiches gilt für die Behörden des Bundesministeriums des Innern, die nicht im Sicherheitsbereich tätig sind.

Für das BfV wird auf den dem Deutschen Bundestag gesondert übermittelten „Geheim“ eingestuftem Antwortteil verwiesen.*

- a) Welche Kosten fielen für eine etwaige Beschaffung an?

Auf die Antwort zu Frage 19 wird verwiesen.

- b) Inwieweit nahm das BMI 2012 eine „Marktbeobachtung“ für „prediktive Software“ oder Software zum „Data Mining“ vor?

Eine Marktbeobachtung für „prediktive Software“ oder Software zum „Data Mining“ erfolgte nicht.

- c) Welche Erkenntnisse wurden hierfür von welcher Abteilung zusammengetragen?

Auf die Antwort zu Frage 19b wird verwiesen.

- d) Was wurde den Landeskriminalämtern hierzu berichtet?

An die Landeskriminalämter wurde hierzu nichts berichtet.

- e) Inwieweit trifft es – wie von BKA-Vizepräsident Prof. Dr. Jürgen Stock auf Fachkonferenzen vorgetragen wurde – zu, dass das BKA jede auf dem Markt befindliche „prediktive Software“ testen würde?

Durch das BKA wurde keine prediktive Software nach der Definition der Fragesteller getestet. Ohne nähere Angaben kann zu Aussagen des Vizepräsidenten des BKA, Dr. Jürgen Stock, leider keine qualifizierte Stellungnahme erfolgen. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

* Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

20. Wann ist die Inbetriebnahme der geheimdienstlichen Datensammlung „NADIS WN“ geplant?

Das „Nachrichtendienstliche Informationssystem“ (NADIS) besteht bereits seit den 70er-Jahren. Mit dem Projekt NADIS (neu) erfolgte eine Anpassung an zeitgemäße Anforderungen im Hinblick auf Handhabung und Funktionalitäten. Nach der Migration des Datenbestandes aus dem Altsystem erfolgte im Juni 2012 die Aufnahme des Wirkbetriebes des neuen NADIS-Systems NADIS WN.

- a) Welche Errichtungsanordnungen werden hierfür überarbeitet, und welchen Stand kann die Bundesregierung hierfür mitteilen?

Die für NADIS WN erforderliche Dateianordnung nach § 14 BVerfSchG wurde vom BMI vorläufig genehmigt.

- b) Welche Firmen haben hierfür Aufträge zur Errichtung des Datenbanksystems sowie für die dort genutzte Software erhalten?
c) Inwieweit kommt in „NADIS WN“ Analysesoftware zum Einsatz?

Für die Antworten zu den Fragen 20b und 20c wird auf den dem Deutschen Bundestag gesondert übermittelten „Geheim“ eingestuftem Antwortteil verwiesen.*

21. Auf welche Art und Weise werden bei Bundesbehörden Informationen in Fall- oder Vorgangsbearbeitungssystemen verarbeitet, die im Zuge von verdeckten Maßnahmen gewonnen wurden?

Die Verarbeitung von im Zuge verdeckter Maßnahmen erlangten Informationen in den Fall- und Vorgangsbearbeitungssystemen des Bundeskriminalamtes und der Bundespolizei sowie in Fallbearbeitungssystemen der Zollverwaltung weicht grundsätzlich nicht von der Verarbeitung offen erlangter Informationen ab. Eine Besonderheit ist, dass Informationen, die im Zuge von verdeckten Maßnahmen gewonnen werden, nach § 101 Absatz 3 StPO entsprechend gekennzeichnet werden.

Durch das BfV werden Informationen, die im Zuge von verdeckten Maßnahmen gewonnen wurden, im Vorgangsbearbeitungssystem des BfV gespeichert.

Die Verarbeitung und Nutzung dieser Informationen erfolgt unter der Maßgabe der zweckgebundenen Zugangsberechtigung durch Vergabe entsprechender Zugriffsrechte. Die Verarbeitung personenbezogener Daten, die durch Maßnahmen nach dem Artikel-10-Gesetz (G 10) bzw. gemäß den §§ 8a Absatz 2 und 2a oder 9 Absatz 4 BVerfSchG erhoben wurden, richtet sich nach § 4 G 10.

- a) Auf welche Weise und in welchem Format werden derart erlangte Informationen aus den Systemen an andere Stellen weitergegeben?

Für das BKA ist die Art der Weitergabe von derart erlangten Informationen abhängig von der Art der betroffenen Datei, in der die Informationen gespeichert sind. Bei Amtsdateien erfolgt die Auskunftserteilung ggf. aufgrund Einzelanfragen auf konventionellem Weg. Bei Verbunddateien bestehen Zugriffsmöglichkeiten durch die in der jeweiligen Errichtungsanordnung bezeichneten Stellen. Eine Auskunftserteilung an Dritte erfolgt hier ggf. aufgrund von Einzel-

* Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

abfragen auf konventionellem Wege oder bei größeren Datenmengen in elektronischer Form.

Die Übermittlung personenbezogener Daten sowie die Datenweitergabe durch die Bundespolizei ist in den §§ 32 bis 33a BPolG geregelt. Weitere Regelungen zur Datenerhebung, -verarbeitung und -nutzung ergeben sich aus dem Abschnitt II (Unterabschnitt 2, Teil 1 und 2) des BPolG.

Durch die Zollverwaltung werden derartige Daten in der Regel papiergebunden, unter Beachtung der gesetzlichen Kennzeichnungspflicht, übermittelt.

Die in dem Vorgangsbearbeitungssystem des BfV gespeicherten Informationen, die im Zuge von verdeckten Maßnahmen gewonnen wurden, werden in der Regel elektronisch nach Maßgabe der in der Antwort zu Frage 21b genannten Vorschriften an andere Stellen übermittelt. Dabei finden die gängigen Formate (Word, PDF, TIF, TXT, Excel) Verwendung. Eine Übermittlung in Papierform ist ebenfalls möglich.

- b) Welche Bestimmungen existieren hierfür hinsichtlich des Datenschutzes?

Grundlage für die Weitergabe von Informationen durch das BKA an andere Stellen sind die Regelungen in den einschlägigen gesetzlichen Übermittlungsvorschriften.

Zudem sind gemäß § 34 BKAG bzw. § 490 StPO in Errichtungsanordnungen jeweils die Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden, zu regeln. In diesen ist den jeweiligen, insbesondere einschränkenden (vgl. z. B. § 477 Absatz 2 StPO) gesetzlichen Vorgaben für eine etwaige Übermittlung von Daten Rechnung zu tragen.

Die Datenverarbeitung, einschließlich der Speicherung durch die Bundespolizei erfolgt nach den Regelungen des BPolG, der StPO und des BDSG. Für die Zollverwaltung richtet sich die Weitergabe von Daten, die durch verdeckte Maßnahmen erlangt wurden, nach dem Zollfahndungsdienstgesetz (ZFdG) sowie nach der StPO. Für Informationen aus verdeckten Ermittlungsmaßnahmen enthält die StPO beispielsweise in § 101 besondere rechtsstaatliche Sicherungen (Kennzeichnungspflicht, Benachrichtigungspflicht, nachträglicher Rechtsschutz, Löschungspflicht). Diese Regelungen werden durch die für das jeweilige Fall- bzw. Vorgangsbearbeitungssystem bestehenden Errichtungsanordnungen und Dienstanweisungen präzisiert und ergänzt.

Aufgrund von Überwachungsmaßnahmen nach dem G 10 bzw. durch Datenerhebungen nach den §§ 8a Absatz 2 und 2a oder 9 Absatz 4 BVerfSchG gewonnene personenbezogene Daten dürfen nur unter den Voraussetzungen des § 4 G 10 übermittelt werden. Die Übermittlung von im Zuge von verdeckten Maßnahmen gemäß § 8 Absatz 2 BVerfSchG gewonnenen Informationen erfolgt nach Maßgabe der Übermittlungsvorschriften des BVerfSchG. Die Übermittlungen unterliegen anlass- oder zufallsbezogenen Kontrollen durch den behördlichen Datenschutzbeauftragten und den BfDI. Überdies wird auf die Kontrollfunktion der G10-Kommission hingewiesen.

22. Welche Regelungen existieren für Fall- oder Vorgangsbearbeitungssysteme hinsichtlich der Anonymisierung von Volltextinformationen?

Konkrete Vorgaben für Anonymisierungen und Löschungen in Fall- oder Vorgangsbearbeitungssystemen der Polizeien des Bundes finden sich in den jeweiligen Errichtungsanordnungen sowie Dienstanweisungen. Diese richten sich

nach den einschlägigen Vorschriften des BKAG, des BPolG, der StPO und des BDSG und werden technisch überwacht und unterstützt.

Konkrete Vorgaben für Anonymisierungen in Fall- oder Vorgangsbearbeitungssystemen des BfV existieren nicht. Personenbezogene Daten, die nicht oder nicht mehr für die Aufgabenerfüllung des BfV erforderlich sind, aber von Daten zu anderen Personen bzw. von Informationen zu Organisationen oder Sachverhalten nicht getrennt und damit nicht gelöscht werden können, unterliegen jedoch auf Grund der einschlägigen Vorschriften einem Nutzungsverbot.

- a) Trifft es zu, dass diese keinen Bezug zu einer bestimmten Person erlauben dürfen?

Werden Vorgänge, Objekte oder Personen gelöscht, können mit diesen verbundene Volltextinformationen nicht abgerufen und somit keine Bezüge zu bestimmten Personen hergestellt werden. Der Löschvorgang für die Volltextinformationen wird automatisiert durchgeführt.

- b) Inwiefern kann die Bundesregierung garantieren, dass dies bei ihren Polizeibehörden vollumfänglich umgesetzt ist?

Die Polizeibehörden des Bundes stellen dies durch technische Maßnahmen sicher.

23. Wie ist die Aussage des BKA-Angehörigen Moritz Aly im Vortrag auf der Veranstaltung Europäischer Polizeikongress am 14. Februar 2012 gemeint, wonach sich die beim BKA bestehenden Datenmengen in den letzten Jahren jährlich verdoppelt hätten?

Die Aussage des BKA-Angehörigen Moritz Aly war eine Reflektion auf die ausschließlich in IDA eingestellten Daten der vergangenen Jahre und diente der Verdeutlichung des kontinuierlichen Anstiegs von polizeirelevanten, digitalisierten Informationen aus exekutiven Maßnahmen des BKA.

- a) Welche Datenbestände sind hiermit gemeint?

Es handelt sich bei den besagten Datenbeständen um Daten, die anhand polizeilicher Maßnahmen des BKA in den letzten Jahren erlangt und mit IDA ausgewertet wurden. Aufgrund der expandierenden Nutzung von digitalen Medien werden in Ermittlungsverfahren zunehmend „digitale Asservate“ sichergestellt, die dann einer Auswertung zuzuführen sind.

- b) Auf welche Untersuchungen oder Prognosen stützt sich Moritz Aly mit der Aussage?

Die besagte Verdopplung erhebt keinen Anspruch auf absolute rechnerische Richtigkeit und spiegelt den ungefähren Trend der vergangenen Jahre wieder. Dies wurde im besagten Vortrag aus Anlass des „Europäischen Polizeikongresses“ von Moritz Aly ausdrücklich betont.

24. Inwieweit nutzen Bundesbehörden in Ermittlungsverfahren Bilder aus der Satellitenaufklärung?

Bilder aus der Satellitenaufklärung werden im BKA anlassbezogen zur Objektaufklärung, zur Vorbereitung von Exekutivmaßnahmen und zur Aufklärung von Tatorten bspw. bei Anschlägen gegen die Bundeswehr oder Tötungsdelikten zum Nachteil deutscher Staatsangehöriger in Afghanistan genutzt. Die Bundes-

polizei und die Zollverwaltung nutzen in Ermittlungsverfahren keine Satellitenaufklärung.

- a) Welche zivilen oder militärischen Behörden oder Firmen werden hierfür angefragt?

Ansprechpartner für das BKA ist das Zentrum für satellitengestützte Kriseninformationen (ZKI) beim Deutschen Zentrum für Luft- und Raumfahrt e. V. (DLR). Für Ermittlungen in Afghanistan wurden militärische Satellitenaufnahmen verwendet. Diese Aufnahmen wurden im Rahmen der Amtshilfe durch die Bundeswehr zur Verfügung gestellt.

- b) Wie beurteilt die Bundesregierung die gegenwärtige Qualität und Aussagekraft derartiger Satellitenbilder?

Die gegenwärtige Qualität ist nach Einschätzung des BKA noch zu gering, um tatsächliche Aussagekraft mit direktem (kriminal-)polizeilichem Nutzen zu entfalten.

- c) Wie beurteilt die Bundesregierung den Nutzen der genutzten Satellitenbilder für die jeweiligen Ermittlungsverfahren?

Die Satellitenaufnahmen zur Aufklärung von Straftaten in Afghanistan geben dem BKA einen Überblick über die Tatorte.

- d) Wie beurteilt die Bundesregierung einen etwaigen Nutzen der Satellitenbilder auch zur Gefahrenabwehr?

In Einzelfällen werden Satellitenbilder zur Gefährdungs- und Lageeinschätzung im Ausland herangezogen, wenn z. B. die Region aufgrund politischer oder topographischer Gegebenheiten außerhalb staatlicher Kontrolle liegt.

- e) Für welche Zwecke hält die Bundesregierung den Einsatz von Satellitenaufklärung für zweckmäßig und sinnvoll?

Aus den in der Antwort zu Frage 24d genannten Gründen könnte ein Einsatz von Satellitenaufklärung auch in konkreten Ermittlungsverfahren von Bedeutung sein (z. B. bei Straftaten nach dem Völkerstrafgesetzbuch), wenn in den betreffenden Staaten z. B. auf Grund kriegerischer Auseinandersetzungen keine zeitnahe Tatortarbeit möglich ist.

25. Auf welche Art und Weise ist die Bundesregierung am EU-Forschungsprogramm „Composite“ beteiligt, bzw. welche Beiträge mit welchem Inhalt wurden hierfür erbracht (Antworten auf Fragebögen bitte als Anlage beifügen)?

Bei COMPOSITE handelt es sich um ein Sicherheitsforschungsprojekt, das im Rahmen des 7. EU-Forschungsrahmenprogramms von der EU gefördert wird. Weder die Bundesregierung noch nachgeordnete Behörden sind an dem Projekt beteiligt. Beiträge zu diesem Projekt wurden seitens des Bundes bisher nicht erbracht.

26. Inwieweit will Europol die Suche nach allgemeinen und spezifischen „(Bedrohungs-)Indikatoren“ mit der „EU-SOCTA-Methode“ automatisieren?

Europol führt keine automatisierte Suche nach allgemeinen und spezifischen Indikatoren durch. Die einzelnen Indikatoren wurden durch Europol mit den Mitgliedstaaten erarbeitet, durch das „Comité de Sécurité Intérieure“ [CoSI] verabschiedet und sind Gegenstand der durch Europol an die Mitgliedstaaten versandten Fragenkataloge zur Datenerhebung für den SOCTA. Die dem SOCTA zu Grunde liegenden Informationen basieren insoweit primär auf Zulieferungen der EU-Mitgliedstaaten und der sonstigen EU-Agenturen hinsichtlich OK-Gruppen [OC groups], Kriminalitätsphänomenen [SOC areas] und Umfeldfaktoren. Ferner werden die bei Europol bereits vorliegenden Informationen sowie Erkenntnisse aus sog. Open-Source-Recherchen von Europol berücksichtigt.

Ergänzt werden die Zulieferungen durch Einschätzungen der Mitgliedstaaten zu kriminalitätsbeeinflussenden Faktoren [crime relevant factors]. In diesem Punkt werden insbesondere die Ergebnisse einschlägiger wissenschaftlicher Studien herangezogen.

- a) Auf welche technische Art und Weise soll die „Trendanalyse“ bewerkstelligt werden?
- b) Welche Behörden, Unternehmen oder sonstigen Personen sind an der Entwicklung beteiligt?
- c) Welche Datenquellen würde die „EU-SOCTA-Methode“ auswerten?

Auf die Antwort zu Frage 26 wird verwiesen.

- d) Aus welchen deutschen Datensammlungen könnten hierfür (statische) Daten angeliefert werden?

Das BKA bedient die Informationsbedürfnisse Europols zur Erstellung des SOCTA im Wesentlichen mit strategischen Informationen aus dem Bundeslagebild Organisierte Kriminalität, den Daten der sonstigen Bundeslagebilder aus dem Spektrum der Schweren und Organisierten Kriminalität sowie mit Daten der Polizeilichen Kriminalstatistik. Hinsichtlich kriminalitätsbeeinflussender Faktoren und Umfeldaspekten werden die Ergebnisse wissenschaftlicher Studien an Europol übermittelt.

- e) Was ist mit der betriebenen Identifizierung von „Crime Relevant Factors“ gemeint?

Kriminalitätsbeeinflussende Faktoren sind gemäß Definition von Europol „Entwicklungen in der Gesellschaft, die einen wichtigen Einfluss auf die unterschiedlichen Aspekte der schweren und organisierten Kriminalität, einschließlich der Kriminalitätsbereiche, und das Verhalten sowohl der kriminellen Akteure als auch der Opfer ausüben“. Kriminalitätsbeeinflussende Faktoren umfassen Unterstützungsfaktoren (z. B. der zunehmende Zugang zum Internet) und Schwachstellen innerhalb der Gesellschaft, die Gelegenheiten zur Tatbegehung bzw. Chancen zur Kriminalitätsbekämpfung schaffen. Kriminalitätsbeeinflussende Faktoren schließen alle Umfeldaspekte mit ein. Die CRF werden durch Europol als Kriterien für die Priorisierung von Lageentwicklungen herangezogen.

- f) Inwieweit soll dadurch eine Priorisierung von Kriminalitätsbereichen vorgenommen werden?

Die Auswertung der erhobenen Informationen wird durch Europol im Rahmen der Erstellung des SOCTA 2013 erfolgen. Der Bericht wird im Verlauf des ersten Halbjahrs 2013 fertig gestellt. Zur Priorisierung einzelner Kriminalitätsbereiche kann erst nach Abschluss des Prozesses und nach einer Evaluierung der Prioritätensetzung durch das „Comité de Sécurité Intérieure“ (CoSI) Stellung genommen werden.

27. Welche „Anwendungstools“ werden den Teilnehmern/Teilnehmerinnen des Lehrgangs „Grundlagen und Methoden der polizeilichen Informationsverarbeitung“ (Operative Analyse) – wie im Falle von Polizeiangehörigen aus Weißrussland – „mit Hilfe der Software Analyst’s Notebook“ vorgeführt (Bundestagsdrucksache 17/10713)?

Es wurden einfache Anwendungen der in der Software vorhandenen Beispiele gezeigt, wie z. B. Diagrammtechniken, in denen sowohl Verbindungen als auch eine Zeitleiste zusammen dargestellt werden (Kombination aus Relations- und Flussdiagramm); weiterhin die Suchmöglichkeiten nach Entitätsentsprechungen, automatisierte Diagrammlayouts (kreisförmig, gruppiert, hierarchisch, organisatorisch, Fächer) und OLE-Varianten (Object Linking and Embedding). Es handelt sich um ein Verfahren zur Nutzung von Daten aus anderen Anwendungen. Die Daten werden als OLE-Objekte bezeichnet. In Analyst’s Notebook kann man Daten in ein Diagramm einfügen, die in einer anderen Windows-Anwendung erstellt wurden (z. B. eine Excel-Tabelle oder ein Word-Dokument). Sie verhalten sich ebenso wie andere Diagrammelemente, da sie Karten und Identitäten besitzen und mit anderen Diagrammelementen verknüpft werden können. Umgekehrt kann man Diagramme in andere Windows-Anwendungen einfügen. Man kann beispielsweise Teile eines Diagramms kopieren und in ein Word-Dokument oder Paint-Bild einfügen. Informationen der Abschlussübung wurden strukturiert in dem Textverarbeitungsprogramm Editor eingetragen und anschließend etappenweise importiert, so dass sukzessive in relativ kurzer Zeit eine gut erkennbare Grafik entwickelt werden konnte.

- a) Auf welche Art und Weise werden Ermittlungen derart visualisiert, und welchen Vorteil haben Behörden hiervon?

Es ist nach wissenschaftlichen Erkenntnissen für den Menschen einfacher, Erkenntnisse aus visualisierten Informationen zu gewinnen, als dies beispielsweise beim Lesen von Texten oder Zahlen möglich ist. Visualisierungen finden daher vielfach Anwendung, z. B. mittels sog. bildgebender Verfahren. Ein bildgebendes Verfahren erzeugt aus Messgrößen eines realen Objektes ein Abbild, wobei die Messgröße oder eine daraus abgeleitete Information ortsaufgelöst und über Helligkeitswerte oder Farben kodiert visualisiert wird. Zur Visualisierung im Rahmen von Ermittlungen werden gewonnene Informationen zunächst in einer Datenbank erfasst. Die einzelnen Informationen wurden zuvor einer Bewertung unterzogen, die sich im Ergebnis aus Informationsquelle und Informationsgenauigkeit (Entfernung der Quelle zur Information) zusammensetzt. Darüber hinaus werden die Informationen in Beziehung zueinander gesetzt, sofern vorhanden bzw. bekannt. Die Software bietet letztendlich die Möglichkeit, die verschiedenen Informationen und deren Beziehungen zueinander grafisch darzustellen, indem z. B. jede Information als Objekt und jede Beziehung als Verbindungslinie zueinander dargestellt wird.

b) Was ist mit der „Erstellung von Hypothesen etc.“ gemeint?

Im Lehrgang „Operative Analyse“ wird den Teilnehmenden näher gebracht, wie man aus den strukturierten Ermittlungsinformationen und deren visueller Darstellung Hypothesen bzw. Schlussfolgerungen entwickelt (kriminalistisches Denken). Hypothese, als Vorstufe einer Behauptung, ist dabei eine Aussage, deren Gültigkeit man für möglich hält, die aber nicht bewiesen oder verifiziert ist. Sie stellt somit eine Interpretation unvollständiger, z. T. widersprüchlicher Informationen dar. Sie ist daher eine vorläufige (schwache) Schlussfolgerung, aus der ein Erklärungsversuch bzw. eine Theorie abgeleitet werden kann. Sowohl die Hypothese, als auch die Schlussfolgerung, als Beschreibung der Erkenntnis(se) aus dem Prozess der Verarbeitung von Informationen, bedürfen der Beweisführung und werden auf der Grundlage eines (induktiv- oder deduktiv-)logischen Gerüsts aus den einzelnen Informationen entwickelt.

c) In welchem Umfang wurden auch Behörden aus der Türkei, Russland, der Ukraine, China, Estland, Georgien, Kroatien, Serbien, Aserbaidschan und Montenegro „Analyst’s Notebook“ bzw. ähnliche Analyseprogramme vorgeführt?

Ein Lehrgang „Grundlagen und Methoden der polizeilichen Informationsverarbeitung – Operative Analyse“, bei dem die Vorstellung von Analyst’s Notebook einen Baustein darstellt, wurde durch das BKA seit 2006 in folgenden Staaten durchgeführt:

- Türkei: 6. November bis 8. November 2006 und 12. November bis 19. November 2007
- Ukraine: 15. November bis 20. November 2010 und 25. Mai bis 31. Mai 2011
- Georgien: 8. November bis 13. November 2010.

Im Rahmen des Maßnahmenplans Türkei „Risikoanalyse und Schleusungskriminalität“ haben zwei Beamte der Bundespolizeiakademie im Mai 2010 an einem Erfahrungsaustausch mit 15 Ermittlungsbeamten der türkischen Polizei an der Internationalen Polizeiakademie (TADOC) in Ankara/Türkei teilgenommen. Hierbei wurden Erfahrungen seitens der Bundespolizeiakademie mit den Programmen Analyst’s Notebook und InfoZoom in etwa halbstündigen Vorträgen dargestellt. Eine Schulung der Software erfolgte nicht. Im Rahmen der Ausbildungs- und Ausstattungshilfe, Maßnahmenplan „Georgien“ – Maßnahme 2 – „Risikoanalyse für Grenzpolizei“, 30. August bis 1. September 2011, wurden Erfahrungen seitens der Bundespolizeiakademie mit den Programmen Analyst’s Notebook und InfoZoom in etwa halbstündigen Vorträgen dargestellt. Eine Schulung der Software erfolgte nicht. Am Lehrgang nahmen 20 Angehörige der georgischen Grenzpolizei teil.

