Deutscher Bundestag **Drucksache 18/4193**

18. Wahlperiode 04.03.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/4007 –

Aufrüstung der IT-Analysefähigkeiten bei der EU-Polizeiagentur Europol

Vorbemerkung der Fragesteller

In seinem kürzlich veröffentlichten Arbeitsprogramm für das Jahr 2015 kündigt die Polizeiagentur Europol die Einführung eines ganzen Arsenals neuer Analysesoftware an (Ratsdokument 5250/15). Die Rede ist von „fortgeschrittenen Werkzeugen für Datenverarbeitung, aufklärungsbasierte Analyse, darunter auch strategische Analyse und Analyse offener Quellen“. Schon vor zwei Jahren hatte Europol von Anwendungen zu „Data Fusion“ geschrieben (www.europol.europa.eu/ec3/services). Gemeint ist Data Mining, also die Möglichkeit, die existierenden Datenbestände in Beziehung zu setzen und grafisch anzuzeigen. Die Tageszeitung „THE WALL STREET JOURNAL“ (14. Januar 2013) berichtete darüber hinaus, dass Europol an der Entwicklung neuer digitaler Analysewerkzeuge zur Mustererkennung arbeitet.

Im neuen Arbeitsprogramm werden die Anwendungen als „future-forecasting and scenario techniques“ beschrieben. Es ist aber unklar, inwiefern ihr Einsatz überhaupt rechtlich einwandfrei ist. Data Mining wird von Polizeibehörden in Deutschland beispielsweise nicht vorgenommen (Bundestagsdrucksache 18/707). Auch die neue „Ma³tch“-Technologie zur Echtzeit-Analyse von Finanzdaten, auf deren Einführung Europol drängt, darf vom deutschen Bundeskriminalamt (BKA) nicht angewandt werden (Bundestagsdrucksache 18/2888). Würden aus Deutschland angelieferte Daten bei Europol mit automatisierten Verfahren verarbeitet, könnte es sich nach Ansicht der Fragesteller um einen Verstoß gegen Datenschutzbedingungen handeln. Deutschland ist laut eigenen Angaben „zweitstärkster Nutzer“ von Europols Informationssystemen (Bundestagsdrucksache 18/3766).

Laut dem Arbeitsprogramm sollen Verfahren zur Auswertung und zum Vergleich biometrischer Daten eingeführt werden. Europol beabsichtigt, auf das neue EU-System zur Speicherung von Fingerabdrücken im Schengener Informationssystem zuzugreifen. Auch die Beschaffung von Software zur Erkennung von Personen und Sachen in Bild- und Videodaten steht auf der Europol-Wunschliste. Bald sollen die Arbeiten an einem „European Tracking System“ abgeschlossen sein, mit dem europäische Polizeibehörden ihre GPS-Peilsender (GPS – Global Positioning System), etwa an Fahrzeugen Verdächtiger, auch grenzüberschreitend betreiben können. Europol richtet hierzu einen zentralen Server ein, der außer durch die Mitgliedstaaten auch von „Third Parties“ ge-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 27. Februar 2015 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

nutzt werden kann. Die Ausgabeformate der Peilsender werden hierfür standardisiert. Das seit zwei Jahren bei Europol angesiedelte „European CyberCrime Center“ (EC3) soll einen eigenen „Malware Scanner“ erhalten. Das könnte bedeuten, dass Europol selbst das Internet absucht. Geplant ist auch die Verbesserung des Austauschs in Echtzeit. Nun soll ein übergreifendes „Europol Analysis System“ (EAS) aufgebaut werden. Vor zwei Jahren wurden ähnliche Pläne bekannt, wonach Europol eine „Plattform für den Informationsaustausch von Strafverfolgungsbehörden“ einrichtet (Bundestagsdrucksache 17/13441).

Die Europäische Kommission hat für die Europol-Pläne zusätzliche Mittel von 12,5 Mio. Euro bereitgestellt. Als Begründung der IT-Aufrüstung dient die neue Europol-Verordnung, wonach die Agentur in einem „erweiterten Mandat“ ihre Analysefähigkeiten verbessern und ausweiten soll. Geplant ist etwa, dass Europol zukünftig selbst Daten von europäischen Polizeibehörden einsammeln darf und nicht mehr auf entsprechende Lieferungen warten muss.

1. Inwiefern kann die Bundesregierung ihre Angaben, wonach Deutschland „zweitstärkster Nutzer“ von Europols Informationssystemen ist, nach Zulieferungen und Abfragen aufschlüsseln?

Die Aussage, wonach Deutschland „zweitstärkster Nutzer“ von Europol Informationssystemen ist, bezieht sich im Wesentlichen auf die statistische Auswertung Europols über die Nutzung des „Europol Informationssystems (EIS)“. Mit Stand 6. Januar 2015 waren ca. 236 000 Objekte im EIS gespeichert, wovon aus Deutschland ca. 54 000 Daten zugeliefert wurden. Hiermit ist Deutschland zweitstärkster Zulieferer an das EIS. Im Rahmen der Abfrage von Daten aus dem EIS lag Deutschland mit ca. 13 800 Anfragen im vierten Quartal 2014 zahlenmäßig an dritter Stelle. Die Aussagen beziehen sich lediglich auf die absoluten Zulieferungs- und Abfragezahlen. Sofern man die Häufigkeit von Zulieferungen bzw. Abfragen in Relation zur Einwohnerzahl setzt, liegen weitere Mitgliedstaaten der Europäischen Union (EU) vor Deutschland.

2. Inwiefern hält es die Bundesregierung für notwendig, dass die Polizeiagentur Europol „fortgeschrittene Werkzeuge für Datenverarbeitung, aufklärungsbasierte Analyse, darunter auch strategische Analyse und Analyse offener Quellen“ beschafft, und aus welchem Grund kann dies nicht mit vorhandener IT-Ausrüstung bewerkstelligt werden?

Das Europol insoweit überhaupt IT-Fähigkeiten besitzt, erscheint notwendig. Nach Artikel 5 Absatz 1 Buchstabe a des Europol-Ratsbeschlusses 2009/371/JI hat Europol die Hauptaufgabe Informationen und Erkenntnisse zu sammeln, zu speichern, zu verarbeiten, zu analysieren und auszutauschen. Hierfür unterhält Europol u. a. das Europol Informationssystem (Artikel 11) und Arbeitsdateien zu Analysezwecken (Artikel 14). Europol darf nach Artikel 25 Absatz 4 auch Daten aus öffentlich zugänglichen Quellen direkt einholen und verarbeiten.

3. Was ist der Bundesregierung darüber bekannt, welche Anwendungen zur Vorhersage und Szenario-Modellierung („future-forecasting and scenario techniques“) beschafft werden sollen, welche Defizite damit behoben werden sollen und im Rahmen welcher Ermittlungen diese eingesetzt würden?

Der Bundesregierung liegen keine Erkenntnisse darüber vor, welche Anwendungen seitens Europol beschafft und welche Ziele damit verfolgt werden sollen.

4. Was ist der Bundesregierung darüber bekannt, in welchem Maße und in welchen Fällen die aus Deutschland angelieferten Daten bei Europol mit Verfahren zum Data Mining, zur Mustererkennung, zur Prognose oder zu „Predictive Analytics“ verarbeitet werden?

Der Bundesregierung ist nicht bekannt, welche Anwendungen Europol für die konkrete Auswertung einzelner Ersuchen nutzt.

5. Inwiefern kann die Bundesregierung um die Bearbeitung der von ihr angelieferten Daten mit solchen Analyseverfahren bitten oder sie ausschließen?

Ersuchen an Europol werden in der Regel ergebnisorientiert gestellt. Eine Eingrenzung auf bestimmte Analysetools findet nicht statt. Die datenschutzrechtlichen Vorgaben für den Umgang mit deutschen Daten werden durch die Vergabe von so genannten handling codes reguliert.

6. Was ist der Bundesregierung darüber bekannt, in welchem Maße und in welchen Fällen aus Deutschland angelieferte Finanzdaten bei Europol mit der „Ma³tch“-Technologie zur Echtzeit-Analyse analysiert werden, bzw. inwiefern ist ein solches Verfahren geplant?

Das Bundeskriminalamt (BKA) liefert keine Finanzdaten zur Echtzeit-Analyse mit der „Ma3tch“- Technologie an Europol. Der Datenaustausch mit der sogenannten „Financial Intelligence Unit“ (FIU) findet auf direktem Wege – ohne Einbindung von Europol – statt.

Perspektivisch beabsichtigt Europol im Rahmen des EU ISEC-Projekts „FIU.NET: empowering the FIUs and partners in their cross-border cooperation“ (2014 bis 2016) die Implementierung des FIU.net. Ob und in welchem Umfang hierbei die „Ma3tch“-Technologie integriert werden soll, kann nach heutigem Informationsstand noch nicht beurteilt werden.

7. Inwiefern bzw. auf welcher rechtlichen Grundlage hält die Bundesregierung ein solches Verfahren für denkbar, obwohl dies dem deutschen BKA untersagt ist?

Das BKA prüft derzeit, ob und gegebenenfalls unter welchen Maßgaben dieses Verfahren zukünftig angewendet werden könnte.

8. Welche Verfahren zur Auswertung und zum Vergleich biometrischer Daten sollen nach Kenntnis der Bundesregierung bei Europol eingeführt werden?

Derzeit wird von Europol zum Vergleich biometrischer Daten ein AFIS-System eingesetzt. Dieses System soll Ende 2015 durch ein neues System ersetzt werden, technische Details liegen der Bundesregierung derzeit noch nicht vor.

9. Inwiefern beabsichtigt Europol nach Kenntnis der Bundesregierung, auf das neue EU-System zur Speicherung von Fingerabdrücken im Schengener Informationssystem zuzugreifen?

Derzeit erhebt die Europäische Kommission im Rahmen der Prüfung der technischen Umsetzbarkeit den zu erwartenden Durchsatz in einem künftigen SIS II-AFIS. Zu diesem Zwecke wurde an alle europäischen Mitgliedstaaten ein Fragebogen versandt, der die typischen Zugriffsfälle und Häufigkeiten auf ein sol-

ches AFIS erheben soll. Ob dieser auch an Europol versandt und von dort beantwortet wurde, ist der Bundesregierung nicht bekannt.

10. Was ist der Bundesregierung über Pläne Europols zur Beschaffung von Software zur Erkennung von Personen und Sachen in Bild- und Videodaten bekannt, wofür würden diese genutzt, und inwiefern würden auch aus Deutschland gelieferte Daten damit durchsucht?

Am 6. Mai 2014 wurde das BKA durch Europol angefragt, ob dort ein „Fotovergleichs bzw. -identifizierungswerkzeug vorrätig, in der Erprobung oder in Planung ist“. Hintergrund der Anfrage war ein bei Europol stark angestiegenes Datenvolumen insbesondere von Bildern und Videoaufnahmen im Zusammenhang mit der „Syrienreisen-Problematik“. Am 12. Mai 2014 wurde Europol allgemein über die Verfahrensweise des im BKA eingesetzten Gesichtserkennungssystems informiert. Darüber hinaus wurden weitere hier bekannte internationale staatliche Ansprechpartner benannt, die sich mit der Thematik Gesichtserkennung befassen.

Weitere Informationen hinsichtlich der Beschaffung oder möglichen Nutzung einer Software „zur Erkennung von Personen und Sachen in Bild- und Videodaten“ durch Europol liegen hier nicht vor.

11. Was ist der Bundesregierung über den Stand von Arbeiten an einem „European Tracking System“ bekannt, welche Behörden von Mitgliedstaaten der Europäischen Union oder sonstigen Partner sind daran beteiligt, und inwiefern würde das System auch von deutschen Behörden genutzt?

Der Europol-Verwaltungsrat hat im Mai 2014 die Einrichtung des „European Tracking System (ETS)“ als Focal Point befürwortet. Soweit bekannt, ist dies noch nicht erfolgt. Daher stehen auch Beteilige oder Inhalte, anhand deren Deutschland eine Beteiligung prüfen kann, noch nicht fest.

12. Inwiefern werden im Zuge der Errichtung eines „European Tracking Systems“ auch deutsche Ausgabeformate von Peilsendern standardisiert?

Auf die Antwort zu Frage 11 wird verwiesen.

13. Was ist der Bundesregierung darüber bekannt, wofür das bei Europol angesiedelte „European CyberCrime Center“ einen eigenen „Malware Scanner“ erhalten soll?

Die Begrifflichkeit „Malware-Scanner“ ist im BKA nicht bekannt. Seit Dezember 2013 richtete das Europol Cybercrime Centre (EC3) sukzessive ein „Europol-Malware-Analysis-System“ (EMAS) ein, welches inzwischen in den Wirkbetrieb übergegangen ist. Das EMAS ist ein Tool zur Analyse von Malware (Schadprogrammen). Seitens der Mitgliedsstaaten übermittelte Malware-Samples werden einem Abgleich („crossmatching“) mit bereits bekannten Malware-Samples unterzogen und ggf. Bezüge zu anderen Sachverhalten bzw. Fällen aus dem Bereich der Cybercrime hergestellt.

14. Was ist der Bundesregierung darüber bekannt, in welchem Rahmen und auf welcher rechtlichen Grundlage Europol selbst das Internet absucht, etwa zur Auswertung offener Quellen in Sozialen Medien, wie Facebook oder Twitter?

Nach Artikel 25 Absatz 4 des Europol-Ratsbeschlusses 2009/371/JI „kann Europol Daten einschließlich personenbezogener Daten aus öffentlich zugänglichen Quellen, wie beispielsweise Medien, öffentlichen Daten und kommerzielle Informationsanbieter, gemäß den Datenschutzvorschriften dieses Beschlusses direkt einholen und verarbeiten“.

Im Rahmen des Auswerteschwerpunktes „Check-the-Web“ erfolgt auch eine Beobachtung des Internets durch Europol. Insoweit wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/4035 vom 18. Februar 2015 verwiesen.

15. Inwiefern sind die Inhalte bzw. der Umfang der Plattform für den Informationsaustausch bei Strafverfolgungsbehörden (IXP) bei Europol mittlerweile abschließend festgelegt (Bundestagsdrucksache 17/13441)?

16. Welche Informationen zu Behörden, Institutionen, Expertennetzwerken, Strafverfolgungsinstrumenten, Übersetzungswerkzeugen, Kommunikationskanälen sowie Fahndungsdaten soll das IXP nach Kenntnis der Bundesregierung enthalten, und wo wird es angesiedelt?

17. Welche Endnutzer des IXP sind der Bundesregierung bekannt?

Die Fragen 15 bis 17 werden gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung ist eine Realisierung der Information Exchange Platform (IXP) derzeit nicht absehbar. Entsprechende konzeptionelle Vorarbeiten wurden nach Kenntnis der Bundesregierung nicht über den bereits in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/13441 vom 10. Mai 2013 dargestellten Stand hinaus fortgeführt.

18. Was ist nach Kenntnis der Bundesregierung unter dem „Europol Analysis System“ zu verstehen, und welche Fähigkeiten bzw. Anwendungen werden hierunter zusammengefasst?

Beim „Europol Analysis System“ (EAS) handelt es sich um eine Plattform, auf der die bei Europol eingesetzten Analysetools gesammelt sind. Hauptaufgabe des EAS ist die Unterstützung der operativen und strategischen Analyse durch Europol. Als Kernkomponente des „Europol Analysis System“ sind die Arbeitsdateien für Analysezwecke (Artikel 14 des Europol-Ratsbeschlusses 2009/371/JI) zu nennen.

19. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit, derartige Analysetätigkeiten in der neuen Europol-Verordnung zu verankern?

Die Bundesregierung befürwortet, dass Europol grundsätzlich personenbezogene Daten zum Zweck der strategischen oder themenbezogenen Analyse verarbeiten darf. Im Standpunkt des Rates zu Artikel 24 Absatz 1 Satz 2 Buchstabe b des Entwurfs der Europol-Verordnung finden sich entsprechende Regelungen, die im laufenden europäischen Gesetzgebungsverfahren weiter beraten werden.

20. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit, die neue Europol-Verordnung so zu gestalten, dass Europol selbst Daten einsammeln kann und nicht mehr auf Zulieferungen der Mitgliedstaaten warten muss?

Die Bundesregierung befürwortet, dass Europol in der Regel ausschließlich Informationen verarbeiten darf, die ihm übermittelt werden, wie es der Standpunkt des Rates zu Artikel 23 Absatz 1 des Entwurfs der Europol-Verordnung vorsieht.

Daneben soll Europol Informationen einschließlich personenbezogener Daten aus öffentlich zugänglichen Quellen wie dem Internet sowie öffentliche Daten direkt einholen und verarbeiten können, wie es der Standpunkt des Rates zu Artikel 23 Absatz 2 des Entwurfs der Europol-Verordnung vorsieht.

Eine vergleichbare Möglichkeit besteht bereits nach Artikel 25 Absatz 4 des Europol-Ratsbeschlusses 2009/371/JI. Auf die Antwort zu Frage 14 wird verwiesen.

21. Welche Position vertritt die Bundesregierung hinsichtlich der Möglichkeit direkter Kontakte zwischen Europol und nationalen Behörden unter Umgehung des bislang vorgeschriebenen Weges über die jeweilige nationale Kontaktstelle?

Die Bundesregierung befürwortet, dass die Mitgliedstaaten vorbehaltlich der von ihnen jeweils festgelegten Voraussetzungen, einschließlich einer vorherigen Einbeziehung der nationalen Stelle, direkte Kontakte zwischen ihren zuständigen Behörden und Europol gestatten können, wie es der Standpunkt des Rates zu Artikel 7 Absatz 4 des Entwurfs der Europol-Verordnung vorsieht.

Eine vergleichbare Möglichkeit direkter Kontakte besteht bereits nach Artikel 8 Absatz 2 des Europol-Ratsbeschlusses 2009/371/JI.

22. Mit welchen „als relevant eingeschätzten Bedrohungslagen und Sachverhalten aus dem Bereich der Cybercrime“ hat sich die „Joint Cybercrime Action Taskforce“ (J-CAT) nach Kenntnis der Bundesregierung „bedarfs- und anlassbezogen“ befasst (Bundestagsdrucksache 18/2674)?

Die Joint Cybercrime Action Task Force (J-CAT) war mit folgenden relevanten Bedrohungslagen bzw. Sachverhalten befasst:

Im Rahmen der Operation ONYMOUS – Hauptziel dieser Operation war die Plattform Silk Road 2.0 – war die J-CAT insbesondere an der Koordinierung von Exekutivmaßnahmen beteiligt. Im Rahmen der Ermittlungen wurden über 100 weitere illegale Services identifiziert und im Rahmen eines koordinierten Takedowns am 6./7. November 2014 abgeschaltet. Beteiligt waren 15 Länder (Bulgarien, Tschechien, Finnland, Frankreich, Ungarn, Lettland, Litauen, Luxemburg, Niederlande, Rumänien, Spanien, Schweden, Schweiz, UK, Deutschland).

Maßnahmen im Rahmen der OP IMPERIUM zielten auf bulgarische, organisierte Tätergruppierungen ab, die Skimming-Straftaten in ganz Europa durchführten. Am 30. September 2014 fanden Festnahmen in Spanien und Bulgarien statt.

23. Welche Rolle kam dabei jeweils Europol zu?

Europol nahm in den Sachverhalten eine koordinierende Rolle ein.

24. Auf welche Weise haben sich „Cybercrimedienststellen aus den USA, Kanada, Australien und Kolumbien“ in die Arbeit des J-CAT eingebracht?

Die genannten vier Nationen sind im J-CAT vertreten. Es erfolgt ein anlassbezogener Informationsaustausch.

25. Mit welchen Aufgaben war der vom BKA für die sechsmonatige Pilotphase von J-CAT entsandte Mitarbeiter bislang befasst?

Zu den Aufgaben des Mitarbeiters des BKA zählte der anlassbezogene Informationsaustausch mit den anderen Teilnehmern des J-CAT und die Abklärung und Rückkopplung von Informationen an die Heimatdienststelle.

26. Inwiefern wurden bereits „auf Grundlage von Auswertungen koordinierte Maßnahmen gegen Hauptakteure und Erscheinungsformen aus dem Phänomenbereich Cybercrime“ betrieben, indem Ermittlungsverfahren auf nationaler Ebene eingeleitet wurden?

Derartige Ermittlungsverfahren wurden bislang nicht eingeleitet.

27. Inwiefern wurde bei den Ermittlungen außer auf die Focal Points „Cyborg“, „Terminal“ und „Twins“ auf weitere „bei Europol vorliegende[n] Informations- und Auswertemöglichkeiten“ zurückgegriffen?

Die Inanspruchnahme von Ressourcen aufseiten von Europol beschränkt sich auf die Einbindung der genannten Focal Points.

28. Was ist der Bundesregierung über Ziele und Beteiligte einer „European Expert Group on Cybercrime“ bekannt?

a) Wer führt die Gruppe an, und welche Rolle übernehmen die „Leader“ und „Co-Leader“ (bitte für eine etwaige deutsche Beteiligung ausführlich darstellen)?

Die Fragen 28 und 28a werden gemeinsam beantwortet.

Die Maßnahme zur Gründung bzw. Etablierung der Gruppe wird durch den Aktionsleiter (Leader) Frankreich geführt und durch Co-Aktionsleiter (Co-Leader) Europol und Deutschland (Bundeskriminalamt und bayerisches Landeskriminalamt) unterstützt. Weitere Mitgliedstaaten der EU und EU-Agenturen sind Teilnehmer der Maßnahme. Der Aktionsleiter ist insbesondere für die Koordination der Aktivitäten der Teilnehmer an der Maßnahme verantwortlich. Daher soll er sich mit den Co-Aktionsleitern zur weiteren Gestaltung der Maßnahme abstimmen und weitere Teilnehmer einbinden.

b) Wann und auf wessen Veranlassung wurde die Gruppe gegründet?

Die Gründung bzw. Etablierung der Gruppe ist Ziel einer Maßnahme, die im Rahmen der internationalen Zusammenarbeit des EU Policy-Cycle in der Priorität „Cyber-Attacks“ (Cyberangriffe) im operativen Aktionsplan (OAP) Cyber-Attacks für das Jahr 2015 beschlossen wurde.

c) Auf welche Art und Weise und mit welcher Zielsetzung werden in der „European Expert Group on Cybercrime“ auch Anonymisierungsverfahren und Verschlüsselungen behandelt?

Der Austausch von Erfahrungen im Bereich Cyberangriffe soll wesentlicher Bestandteil der Gruppe sein. In diesem Rahmen können alle strafrechtlich relevanten Themenfelder, so auch Anonymisierungsverfahren und Verschlüsselung, bedarfs- und anlassbezogen mit einbezogen werden.

d) Welchen ähnlichen EU-Arbeitsgruppen gegen „Cyberkriminalität“ gehören deutsche Behörden als „Leader“, „Co-Leader“ oder Unterstützer an?

In der Priorität Cyberangriffe sind in dem operativen Aktionsplan 2015 weitere Maßnahmen mit deutscher Beteiligung geplant, in denen Deutschland als Aktionsleiter, Co-Aktionsleiter oder Teilnehmer fungiert. Die Umsetzung dieser Maßnahmen kann auch in Form von Arbeitsgruppen erfolgen.

29. Auf welche Weise wurde nach Kenntnis der Bundesregierung das Projekt „Interpol project on interoperability – A practical development for enhanced police cooperation within EU Member States“ inzwischen weiterbetrieben oder umgesetzt (Ratsdokument 10094/14)?

Soweit bekannt wurde das oben genannte Projekt durch Interpol Ende 2014/Anfang 2015 bei der EU eingereicht, um sich für eine Finanzierung zu bewerben. Die Frist zur Einreichung von Projektvorschlägen bei der Europäischen Union endete am 14. Januar 2015. Weitere Informationen zur Umsetzung des erwähnten Projektes liegen der Bundesregierung nicht vor.

a) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus den in dem Dokument genannten Defiziten sowie den dort gemachten Vorschlägen für den Ausbau der polizeilichen Zusammenarbeit?

Die in dem Dokument erwähnten Defizite beziehen sich in erster Linie auf einen vermeidbaren Mehraufwand bei der technischen Verarbeitung von polizeilichen Daten, beispielsweise durch Medienbrüche bei der Nutzung verschiedener Informationskanäle und -systeme.

Inwieweit die Defizite tatsächlich für einzelne bzw. alle Staaten zutreffen, kann von der Bundesregierung nicht beurteilt werden. Zumindest in Deutschland sind das Bundeskriminalamt, die Bundespolizei und die Polizeien der Länder stets daran interessiert, das Prinzip der Interoperabilität beim nationalen bzw. internationalen Informationsaustausch bzw. bei der Datenverarbeitung sicherzustellen. So können im Bundeskriminalamt bspw. durch das dortige Vorgangsbearbeitungssystem nach Eingabe von Personalien bereits zum jetzigen Zeitpunkt und je nach Zugriffsberechtigung mehrere Informationssysteme gleichzeitig bedient werden. Datenschutzrechtliche Restriktionen sind und werden dabei aber stets berücksichtigt.

Grundsätzlich sind die im Bericht gemachten Vorschläge geeignet, die polizeiliche Zusammenarbeit in der EU zu fördern.

b) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung zu der in dem Dokument vorgeschlagenen „One Stop Shopping Strategy“ hinsichtlich deutscher datenschutzrechtlicher Vorgaben?

Wie in der Antwort zu Frage 29 bereits erwähnt, liegen der Bundesregierung keine Detailinformationen zu dem geplanten Projekt vor, daher kann keine abschließende Beurteilung getroffen werden.

Grundsätzlich lässt sich jedoch sagen, dass eine „One Stop Shopping Strategy“ keinen Einfluss auf deutsche datenschutzrechtliche Vorgaben hat.

Datenschutz findet bei der Verarbeitung der Daten und bei der Vergabe der personenbezogenen Zugriffsberechtigungen für polizeiliche IT-Systeme Anwendung. Beides wird auch bei der Umsetzung der „One Stop Shopping Strategy“ berücksichtigt, da die Polizeibediensteten nur auf die Daten zugreifen können, für die sie grundsätzlich berechtigt sind.

30. Was ist der Bundesregierung über die derzeitigen Beteiligten der bei Interpol angesiedelten Projekte VENLIG und HAMAH bekannt, in denen Informationen des US-Verteidigungsministeriums über „ausländische Terroristen“ ausgewertet werden (Bundestagsdrucksache 17/4407)?

a) Was ist der Bundesregierung darüber bekannt, in welchem Umfang VENLIG und HAMAH bzw. ähnliche Projekte für andere Länder überhaupt genutzt werden bzw. inwiefern eine Nutzung seit dem Jahr 2011 zu- oder abnimmt?

Die Fragen 30 und 30a werden gemeinsam beantwortet.

Auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/1411 vom 14. Mai 2014 wird verwiesen.

b) Was ist der Bundesregierung darüber bekannt, ob Europol die dort erlangten Daten nicht nur in die Analysearbeitsdatei „Hydra“ einstellt, sondern auch in anderen Dateien speichert?

Auf die Antwort der Bundesregierung zu Frage 16 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/1411 vom 14. Mai 2014 wird verwiesen.

c) Inwiefern lässt sich rekonstruieren, ob auch deutsche Behörden die aus Beständen des US-Verteidigungsministeriums stammenden Daten abrufen dürfen, bzw. inwiefern ist das Ministerium als Besitzer der Daten erkennbar?

Auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/934 vom 26. März 2014 wird verwiesen.

31. Welche Haltung wird die Bundesregierung in den zuständigen Ratsarbeitsgruppen zur Frage vertreten, ob bzw. mit welchen Einschränkungen Europol, wie im Arbeitsprogramm für das Jahr 2015 skizziert, ein Zusammenarbeitsabkommen mit Israel verhandelt oder abschließt?

Die Bundesregierung hat der Verabschiedung des Europol-Arbeitsprogramms 2015 in der Ratsarbeitsgruppe „Strafverfolgung“ im Januar 2015 zugestimmt. Die Frage, ob bzw. mit welchen Einschränkungen Europol ein Zusammenarbeitsabkommen mit Israel verhandelt oder abschließt, ist nicht thematisiert wor-

den. Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 13 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/3143 vom 4. Oktober 2010 verwiesen.

32. Inwiefern wäre ein solches Abkommen einer EU-Agentur aus Sicht der Bundesregierung überhaupt möglich, wenn dabei mit einer Polizei zusammengearbeitet würde, die über ein Hauptquartier in den von Israel besetzten Gebieten verfügt?

Aus Sicht der Bundesregierung ist ein solches Abkommen zwischen Europol und Israel möglich. Durch eine Territorialklausel kann die Nichtanwendung des Abkommens auf bestimmte Gebiete vorgesehen werden. Ferner kann vorgesehen werden, dass nur solche Informationen nach dem Abkommen verarbeitet werden dürfen, die im Einklang mit internationalem Recht erlangt wurden.

a) Welchen Stand haben nach Kenntnis der Bundesregierung Verhandlungen eines Kooperationsabkommens zwischen Europol und Israel (Bundestagsdrucksache 17/3143)?

b) Welche Informationen sollen im Rahmen des Abkommens getauscht werden?

c) Auf welche Daten hätten israelische Behörden demnach Zugriff?

d) Wie lange würden die Daten in Israel gespeichert?

e) Dürfte Israel die Daten an Drittstaaten weitergeben?

Die Fragen 32a bis 32e werden gemeinsam beantwortet.

Auf die Antwort der Bundesregierung zu Frage 12 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/3143 vom 4. Oktober 2010 wird verwiesen.

33. Was ist der Bundesregierung darüber bekannt, inwiefern die Errichtung und der Betrieb einer gesicherten privaten Kommunikationsinfrastruktur und eine Breitbandverbindung im „sTESTA“-Netzwerk zwischen Estland, Frankreich und Österreich mittlerweile nicht mehr durch ein Konsortium aus OBS (Orange Business Services) und HP (Hewlett-Packard) bereitgestellt wird, sondern auf ein System der Firma T-Systems migriert ist (Bundestagsdrucksache 18/1832)?

Das „sTESTA“-Netzwerk wird weiterhin genutzt. Die Migration auf ein System der Firma T-Systems ist noch nicht abgeschlossen.

34. Welche Gründe sind der Bundesregierung für eine Neuausschreibung des „sTESTA“-Netzwerks bekannt?

Nach Kenntnis der Bundesregierung lief der Vertrag mit dem Betreiberkonsortium für „sTESTA“ aus. Die Europäische Kommission verfolgt unter anderem das Ziel, eine Kommunikationsinfrastruktur für den elektronischen Datenaustausch zwischen etwa 40 Einrichtungen der Europäischen Union und denen der Mitgliedsländer zur Verfügung zu stellen.

35. Was ist der Bundesregierung darüber bekannt, welche technischen Anlagen des SIS I (SIS – Schengener Informationssystem) nach Umstieg auf

das SIS II veraltet sind und nicht mehr genutzt werden, wer für dessen Abbau bzw. Entsorgung zuständig ist und welche Kosten hierfür anfallen?

Der Abbau der technischen Anlagen des SIS 1 und die daraus resultierenden Kosten sind Gegenstand der zuständigen EU-Ratsarbeitsgruppen unter Federführung von Frankreich. Der Abbau und die Entsorgung betreffen alle für SIS 1 genutzten IT-technischen Anlagen. Der Abbau der technischen Gerätschaften zur Unterstützung des SIS 1 wurde zum 29. Oktober 2014 auf Kosten von Frankreich abgeschlossen. Eine Inventarliste wurde unter Anwesenheit von eu-LISA (IT-Agentur der EU) vor der Zerstörung erstellt. Österreich hat den Rückbau für das Backup-System ebenfalls vorgenommen.

36. Inwiefern hat die Bundesregierung mittlerweile weiter geprüft, auf welche Weise ein Europäischer Kriminalaktennachweis (European Police Records Index – EPRIS) etwaige Defizite des grenzüberschreitenden polizeilichen Informationsaustauschs schließen kann (Bundestagsdrucksache 18/1832)?

37. Welche weiteren Schlussfolgerungen zieht die Bundesregierung aus einer hierzu erstellten Studie?

38. Inwiefern und mit welchem (vorläufigen) Ergebnis wurde nach Kenntnis der Bundesregierung in den zuständigen Ratsarbeitsgruppen erörtert, wie etwaige Lücken in den bestehenden polizeilichen Systemen geschlossen werden könnten?

Die Fragen 36 bis 38 werden gemeinsam beantwortet.

Die Ergebnisse der von der Europäischen Kommission im Oktober 2012 vorgelegten Studie „EPRIS“ sind in die Mitteilung der Europäischen Kommission an das Europäische Parlament und den Rat der EU zur „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch“ eingeflossen.

Seither ist das Vorhaben eines Europäischen Kriminalaktennachweises unter französischer Federführung und unter deutscher Beteiligung regelmäßig in der Befassung der Ratsarbeitsgruppe „Informationsaustausch und Datenschutz“ (DAPIX). Hier hat sich gezeigt, dass absehbar nicht mit einem für die Erfüllung der Funktion „Europäischer Kriminalaktennachweis“ ausreichenden Umfang der Nutzung der bestehenden Systeme, hier insbesondere des Europol Informationssystems, zu rechnen ist. Insofern kann nach wie vor von einer funktionalen Lücke in den bestehenden polizeilichen Systemen gesprochen werden.

Im Jahr 2015 wird im Rahmen eines Forschungsauftrages ein Prototyp (Laborsimulation) zur daten- und geheimschutzfreundlichen Nutzung von Daten in dezentralen Systemen entwickelt. Auf dieser Grundlage werden rechtliche und technische Aspekte eines Europäischen Kriminalaktennachweises weiter geprüft werden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333