Deutscher Bundestag **Drucksache 18/11661**

18. Wahlperiode 23.03.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/11395 –

Standardisierung europäischer Informationssysteme

Vorbemerkung der Fragesteller

Unter Leitung des Bundeskriminalamtes arbeiten Europol, Interpol und einige Mitgliedstaaten seit 2007 an einem „Universellen Nachrichtenformat“ („Universal Message Format“, UMF) für einen „verbesserten automatisierten Informationsfluss“ (Bundestagsdrucksache 18/8323). Das UMF soll zum Standard für sämtliche Daten zu Personen und Sachen in den europäischen Informationssystemen werden. Zusammen mit der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA) sollen Europol und Interpol außerdem prüfen, unter welchen Voraussetzungen die dort geführten Informationssysteme in Abfragen eingebunden werden könnten. Europol betreibt hierfür bereits ein Pilotprojekt unter dem Namen „Querying Europol Systems“ (QUEST). Ein ähnliches Pilotprojekt wird bereits von einigen EU-Mitgliedstaaten sowie Europol unter dem Namen „Automatischer Daten Austausch Prozess“ (ADEP) betrieben. Ziel ist die Entwicklung einer Anwendung, um anhand von Suchkriterien festzustellen, in welchem Mitgliedsland der EU „mit sehr hoher Wahrscheinlichkeit polizeiliche Informationen zu einer bestimmten Person vorliegen“ (Bundestagsdrucksache 18/8323). Schließlich werden die Partner des sogenannten Prüm-Verbundes von der Europäischen Kommission aufgefordert, zu prüfen, ob die nationalen Biometrie-Datenbanken auf EU-Ebene angesiedelt werden könnten (http://gleft.de/1BX). Weitere Möglichkeiten zur Verbesserung des europäischen Datentauschs soll die im Sommer 2016 gestartete „hochrangige Sachverständigengruppe für IT-Systeme und Interoperabilität“ erarbeiten. Im Dezember 2016 hat die Gruppe einen Zwischenbericht veröffentlicht. Der eigentlich für Juli 2017 angekündigte Abschlussbericht wurde auf April dieses Jahres vorgezogen.

Vorbemerkung der Bundesregierung:

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage 13e nicht erfolgen kann. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegen-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 21. März 2017 übermittelt.

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

über der Bundesregierung wird insoweit durch gleichfalls Verfassungsrang genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Die o. g. Frage zielt im Kern auf die Offenlegung bestimmter nachrichtendienstlicher Arbeitsmethoden und Vorgehensweisen. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) jedoch besonders schutzwürdig. Das Bekanntwerden der näheren Umstände hierzu könnte das Wohl des Bundes gefährden. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren und daher in einer zur Veröffentlichung vorgesehenen Fassung nicht behandelt werden können. Mit einer substantiierten Beantwortung dieser Frage würden Einzelheiten zur Arbeitsweise und Methodik des Bundesnachrichtendienstes (BND) benannt, die die weitere Funktionsfähigkeit und Aufgabenerfüllung auf dem spezifischen Gebiet der technischen Aufklärung gefährden würden. Eine Auflistung der konkreten Arbeitsweise bzw. -mittel für den Empfang von Daten aus der technischen Aufklärung würde weitgehende Rückschlüsse auf die Arbeitsmethodik, technische Ausstattungen und Möglichkeiten und somit mittelbar auch auf das Aufklärungsprofil des Bundesnachrichtendienstes zulassen, so dass unmittelbare, schutzwürdige Geheimhaltungsinteressen berührt sind. Dadurch könnte die Fähigkeit des BND, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung und Funktionsfähigkeit des Bundesnachrichtendienstes jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Zur Erstellung möglichst vollständiger Lagebilder und zur Vermeidung von Informationsdefiziten ist der Bundesnachrichtendienst auf die aus der technischen Aufklärung zu generierenden Informationen angewiesen. Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen technischen Fähigkeiten des Bundesnachrichtendienstes bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und technische Fähigkeiten des Bundesnachrichtendienstes gewinnen.

Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des BND – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 BNDG) – nicht mehr sachgerecht erfüllt werden könnte.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung des Bundesnachrichtendienstes nicht in Betracht, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Die angefragten Inhalte beschreiben die technischen Fähigkeiten des Bundesnachrichtendienstes so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Dies gilt umso mehr, als sie Spezifika betreffen, deren technische Umsetzung nur in einem bestimmten Verfahren erfolgen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse des Bundesnachrichtendienstes zurückstehen.

1. Im Rahmen welcher Forschungen oder Pilotprojekte auf europäischer Ebene befassen sich welche Behörden des Bundesministeriums des Innern (BMI) mit dem verbesserten Datentausch, der „Interoperabilität“ von Informationssystemen der Europäischen Union, dem Prinzip „One-Stop-Shop“ sowie der Suche nach „Kreuztreffern“, bzw. welche Änderungen haben sich diesbezüglich zur Bundestagsdrucksache 18/8323 ergeben?

Das Bundesministerium des Innern (BMI) ist mit einem Vertreter an der High Level Expert Group (HLEG), die sich u. a. mit den Themen „Interoperabilität“, „One-Stop-Shop“ und Suche nach „Kreuztreffern“ befasst, beteiligt.

2. Welche Fortschritte sind der Bundesregierung zum Projekt „Universal Message Format“ (UMF 3) zur Standardisierung von Anfragen an nationale Polizeisysteme der EU-Mitgliedstaaten und an internationale Systeme wie z. B. das Europol Information System (EIS) bekannt?

Das UMF3 (Universal Message Format) Projekt befindet sich im vorgesehenen Zeitplan. Strukturell besteht das Projekt aus 3 Teilen:

- Teil 1: Erweiterung des UMF-Standards:
  Die vorherige Version 1.0 wurde in der Zwischenzeit auf Version 1.1 erweitert.
- Teil 2: Organisationsform („Governance“):
  Ein Vorschlag, der in der Folge noch mit den verantwortlichen Partnern diskutiert werden wird, wird Ende März eingebracht werden.
- Teil 3: Pilotprojekte mit Einbindung von Europol und fünf EU-Mitgliedstaaten:
  Die Vorbereitungen für die Implementierungen laufen. Die Kommunikation zwischen Europol und den EU-Mitgliedstaaten wird via eines REST-Service realisiert. Der interne Name dafür ist bei Europol QUEST. Europol bereitet derzeit eine Testplattform vor, die von den EU-Mitgliedstaaten für die Tests verwendet wird. Das Testverfahren ist mehrstufig, die Tests werden daher auch abhängig vom Fortschritt der Arbeiten in den EU-Mitgliedstaaten, die nächsten Monate andauern. Die Aufnahme des Wirkbetriebs von QUEST ist noch für 2017 geplant.

a) Welche europäischen Informationssysteme oder Datenbanken arbeiten nach Kenntnis der Bundesregierung bereits nach dem UMF-3-Standard?

Grundsätzlich ist festzuhalten, dass UMF ein flexibler, systemunabhängiger Standard zur Übermittlung von Informationen ist.

Nach den vorliegenden Informationen wird UMF von FRONTEX für den Informationsaustausch mit Europol genutzt. Weiterhin kann von den Mitgliedstaaten für den Prüm-Nachfolgeschriftverkehr seit 2014 ein UMF-konformes, mehrsprachiges, elektronisches Formular verwendet werden, wenn es ihre technische Infrastruktur erlaubt.

Die weitere Nutzung von UMF im Echtbetrieb wird derzeit mit dem Teilprojekt 3 in Verbindung mit QUEST umgesetzt.

b) Was ist der Bundesregierung darüber bekannt, wann bei Europol der Webservice „QUEST“ in Betrieb gehen soll?

Auf die Antwort zu Frage 2 wird verwiesen.

c) Auf welche Weise soll auch „QUEST“ UMF-kompatibel werden?

QUEST wird Auskünfte aus dem Europol Information System (EIS) standardisiert und gemäß den Spezifikationen des aktuellen UMF Standards an den Anfragenden übermitteln. Damit können die Informationen rasch und mit hoher Genauigkeit weiterverarbeitet bzw. weitergeleitet werden.

3. Mit welchem Ergebnis wurde in dem Pilotprojekt „Pilot Programme for Data Exchange of the Passenger Information Units“ (PNRDEP) Möglichkeiten der Vernetzung der nationalen PNR-Zentralstellen und des Austauschs der PNR-Daten untereinander untersucht bzw. gefunden (Bundestagsdrucksache 18/8323)?

Deutschland ist kein Projektpartner im von Ungarn initiierten PNRDEP (Passenger Name Records Data Exchange Programme) Projekt. Im Rahmen der Informal Working Group on PNR (IWG-PNR) am 7. März 2017 stellte Ungarn kurz den Sachstand zum PNRDEP Projekt dar. Demnach dauert das Projekt noch an. Aktuell werden im Projekt verschiedene Varianten für die Kommunikation der Passenger Information Units (PIUs) u. a. über das von Europol entwickelte Kommunikationssystem SIENA (Secure Information Exchange Network Application) getestet. Das Ergebnis des Projektes soll allen EU-Mitgliedstaaten auf einer PNRDEP Abschlussveranstaltung im Juni 2017 vorgestellt werden.

a) Was ist der Bundesregierung darüber bekannt, welche Technologie bereits bestehender Informationssysteme für das Projekt PNRDEP eingesetzt werden soll?

Welche konkrete Technologie bereits bestehender Informationssysteme im PNRDEP getestet werden, ist der Bundesregierung nicht bekannt. Bei der Vorstellung des Projektes wurde lediglich beispielhaft auf einen Test für die Kommunikation der PIUs untereinander mittels des Kommunikationssystems SIENA mit einem extra entwickelten Formular als Anlage verwiesen.

b) Welche bereits vorhandenen Netzwerke, etwa das polizeiliche SIRENE-Netzwerk oder das bei Europol angesiedelte Netzwerk für Finanzermittlungen bzw. das bei Europol eingerichtete SIENA-Netzwerk, könnten aus Sicht der Bundesregierung für den Informationsaustausch unter den PNR-Zentralstellen genutzt werden?

Die Europolkommunikationsplattform SIENA wird favorisiert und entsprechend im europäischen Kontext beworben. Eine abschließende Abstimmung mit den europäischen Partnern steht noch aus. Zudem wird international diskutiert, inwieweit der Informationsaustausch bei verifizierten Treffern (nach einem Abgleich der Passagierdaten mit dem SIS II Bestand) über das SIRENE-Netzwerk durchzuführen ist.

c) Inwiefern hält es die Bundesregierung für technisch möglich, zur Verarbeitung von Daten des EU-PNR die sogenannte Ma3tch-Technologie (Autonomous Anonymous Analysis) zu nutzen?

Die Niederlande haben einen Projektantrag im Rahmen eines „ISF-Calls“ (Internal Security Fund) zur Vernetzung der PIUs eingereicht, in welchem ein möglicher Datenabgleich der PIUs untereinander über die Ma3tch-Technologie unter dem Arbeitsnamen PIU.net geprüft werden soll. Falls das Projekt von der Europäischen Kommission angenommen wird, plant Deutschland an diesem Projekt als „Observer“ teilzunehmen.

d) Was kann die Bundesregierung zu einem Pilotprojekt „PIU net“ mitteilen, das von Behörden der Niederlande, Deutschlands, Großbritanniens und der Vereinigten Staaten von Amerika durchgeführt wird (Ratsdokument 12204/16)?

Auf die Antwort zu Frage 3c wird verwiesen.

e) Inwiefern sind der Bundesregierung mittlerweile die Kosten und die teilnehmenden Drittparteien von PNRDEP bekannt geworden?

In das PNRDEP Projekt sind neben Ungarn auch Bulgarien, Litauen, Portugal, Rumänien und Spanien involviert. Europol ist assoziierter Partner. Die bisherigen Kosten des Projekts sind der Bundesregierung nicht bekannt.

f) Welche drei Pilotprojekte werden an den Flughäfen in Hamburg, Berlin-Schönefeld und Köln/Bonn durchgeführt, bei denen unter anderem Passagierkontrollen und Einsatz des Sicherheitspersonals optimiert werden sollen (airliners.de vom 17. Februar 2017, „Bundespolizei mahnt mehr Sicherheit an deutschen Airports an“)?

Das BMI und der Bundesverband der Deutschen Luftverkehrswirtschaft (BDL) haben im August 2013 zusammen ein Projekt zur Prozessoptimierung der Passagiersteuerungs- und Sicherheitskontrollverfahren initiiert. Dabei soll der gesamte Prozess beginnend von der Flugbuchung bis zum Einsteigevorgang/Abflug umfassend betrachtet und nach Optimierungsmöglichkeiten gesucht werden. Ziel ist, in enger Zusammenarbeit zwischen Luftsicherheitsbehörden, Fluggesellschaften und Flughafenbetreibern einen Gesamtprozess der Passagierabfertigung (auch praktisch) zu erproben, welcher sodann unter Berücksichtigung der flughafen- und standortspezifischen Unterschiede als „best practice“-Modell für künftige Entwicklungen auf europäischer und nationaler Ebene dienen kann.

Das Gesamtprojekt wurde in drei Teilbereichen gebündelt, die an den Standorten Hamburg, Köln-Bonn und Berlin-Schönefeld durchgeführt werden bzw. wurden. Es handelt sich dabei um folgende Teilbereiche:

1. Flughafen Hamburg: Planung und Steuerung der Fluggastströme mit Evaluierung der Auswirkungen auf die Kontrollstelle;
2. Flughafen Köln/Bonn: Konzeption und Verwirklichung einer Kontrollstelle, welche wirtschaftliche Elemente, Sicherheit und Bequemlichkeit für die Passagiere optimieren soll;
3. Flughafen Berlin-Schönefeld: Vertragsgestaltung mit dem Sicherheitsunternehmer.

4. Wann soll das Projekt „Automation of Data Exchange Processes“ (ADEP) von Behörden aus Frankreich (Federführung), Finnland, Irland, Spanien, Deutschland sowie Ungarn (Beobachter) nach Kenntnis der Bundesregierung abgeschlossen sein?

Die Laufzeit orientiert sich an den Vorgaben des einschlägigen EU-Förderprojekts (grundsätzlich ein Jahr mit einer Verlängerungsoption). Das EU-Förderprojekt wurde noch nicht begonnen, ein Projektende ist daher noch nicht definiert.

a) Welche Aufgaben und Arbeiten werden vom Bundeskriminalamt durch die Leitung und die Koordination des Projekts ADEP übernommen?

Das Bundeskriminalamt (BKA) beteiligt sich an dem Pilotbetrieb und berät die Projektleitung hinsichtlich fachlicher und technischer Aspekte.

b) Welche Kosten entstehen für das Pilotprojekt insgesamt, welche Kosten werden von der Bundesregierung und welche von der Europäischen Kommission übernommen?

Die Kosten für das Gesamtprojekt können nicht beziffert werden. Die Europäische Kommission hat eine Förderung in Höhe von 1,5 Mio. Euro für die Entwicklung einer prototypischen Anwendung in Aussicht gestellt, zu weiteren Kosten ist zum jetzigen Zeitpunkt keine Aussage möglich.

c) Mit welchem Ergebnis wurde in ADEP geprüft, ob die „Secure Information Exchange Network Application“ (SIENA), das Europol Information System (EIS) oder die Ma3tch-Technologie, die im FIU-NET (Financial Intelligence Units) Anwendung findet, auch in ADEP eingesetzt werden könnte?

Die genannten Systeme erfüllen nicht die Anforderungen.

d) Aus welchem Grund ist die Ma3tch-Technologie aus Sicht der Bundesregierung hierfür nicht geeignet?

Ziel der Initiative ADEP (Automation of Data Exchange Processes) ist die Entwicklung einer technischen Anwendung, die es (bei Vorliegen eines rechtlich zulässigen Grundes zur Informationserhebung) anhand eng begrenzter Suchkriterien erlaubt, festzustellen, in welchem Mitgliedsland der Europäischen Union (EU) mit sehr hoher Wahrscheinlichkeit polizeiliche Informationen zu einer bestimmten Person vorliegen. Hierdurch soll unter Beachtung der einschlägigen Rechtsvorschriften sodann ein zielgerichteter Informationsaustausch mittels der vorhandenen polizeilichen Kommunikationskanäle initiiert werden.

Gegenstand der Prototyp-Entwicklung ist die Vernetzung dezentraler Datenbestände, um die redundante Speicherung personenbezogener Daten an einer zentralen Stelle zu vermeiden. Zudem erfolgt der Abgleich der Daten ausschließlich in anonymisierter bzw. pseudonymisierter Form. Die hieraus abgeleiteten fachlichen Anforderungen, u. a. an die Grundsätze von „privacy by design“ werden durch die genannte Ma3tch Technologie nicht vollständig abgebildet.

e) Welche dezentralen Datenbestände sollen in ADEP vernetzt werden?

Diese Festlegung obliegt den jeweiligen Pilotteilnehmern. Die Festlegung innerhalb Deutschlands wurde noch nicht final getroffen.

f) Mit welchen Funktionalitäten würde das Bundeskriminalamt Teilnehmer am Pilotverfahren von ADEP?

Das BKA wird Testdaten in pseudonymisierter Form zum Abruf bereithalten und Daten pseudonymisiert abfragen.

5. Was ist der Bundesregierung darüber bekannt, inwiefern die Umsetzung des Vertrages von Prüm auch in der sogenannten European Forensic Science Area (EFSA 2020) behandelt wird?

Der Rat der Europäischen Union hat am 9. Juni 2016 die Schlussfolgerungen und den Aktionsplan im Hinblick auf die Schaffung eines europäischen kriminaltechnischen Raums angenommen (10128/16, EFSA 2020). Der Aktionsplan sieht unter der Maßnahme 6 die Förderung und Verbesserung des Austauschs kriminaltechnischer Daten auf Grundlage der Prümer Beschlüsse vor. Die Maßnahme zielt auf die konsequente Umsetzung der Prümer Beschlüsse sowie auf die Optimierung der Prozesse. Die Federführung zur Umsetzung liegt bei der Ratsarbeitsgruppe DAPIX (Working Party on Information Exchange and Data Protection).

Unter der Maßnahme 2 des Aktionsplanes „Förderung des Austauschs kriminaltechnischer Informationen aus Datenbanken analog zu der im Rahmen der Prümer Beschlüsse 2008/615/JI und 2008/616/JI verwendeten Methodik, mit Schwerpunkt auf Waffen und Munition, Explosivstoffen und Drogen wird zudem folgende Forderung erhoben: „Außerdem muss im Zuge der Perfektionierung von Gesichtserkennungsalgorithmen in einem angemessenen Forum die Möglichkeit erörtert werden, vergleichbare Datenbanken wie für DNA- und Fingerabdruckdaten für diesen zusätzlichen Parameter der biometrischen Identifizierung einzurichten“. Hierzu sind der Bundesregierung aktuell keine Aktivitäten bekannt.

a) Inwiefern sollen hierfür nach Ansicht der Bundesregierung die Übereinstimmungsregeln der Loci angepasst werden?

Mit Entschließung vom 30. November 2009 hat der Rat der Europäischen Union den bis dahin bestehenden „European Standard Set (ESS)“ von 7 auf 12 Merkmalssysteme (oder auch „Loci“) erweitert. Dieser neue Standard wurde auch in Deutschland verbindlich zum 31. Dezember 2010 umgesetzt. Mit der Anpassung sollte auf den künftig verstärkten internationalen Austausch von DNA-Mustern reagiert und die Aussagekraft von DNA-Mustern und Trefferergebnissen verstärkt werden.

b) Was ist der Bundesregierung über Diskussionen zur Aufnahme von Gesichtsbildern in den Abgleich über das Prüm-Verfahren bekannt?

Aus dem Bereich der EU- und Prüm-Zusammenarbeit, insbesondere von Österreich, sind bislang nur sehr allgemeine Vorschläge zur Aufnahme auch von Gesichtsbildern in den Abgleich über das Prüm-Verfahren bekannt. Von einer bereits stattfindenden „Diskussion“ kann hier nicht gesprochen werden.

c) Was ist der Bundesregierung über Pläne bekannt, dass Europol als Prüm-Partner biometrische Daten auch mit Drittstaaten austauschen könnte (Ratsdokument 9368/1/16)?

Europol ist bislang noch kein „Prüm-Partner“. Das genannte Ratsdokument 9368/1/16 sieht hier unter „Action No. 13, Buchstabe c)“ auch zunächst nur vor, eine Aufnahme von Europol als „Prüm-Partner“ zu prüfen. Als Begründung und

Mehrwert wird angeführt, dass es über Europol gelingen könnte, zu bereits erfolgten Prüm-Treffern weitere „cross matches“ auch zu Drittstaaten außerhalb des Prüm-Verbundes herstellen zu können. Zu den Voraussetzungen und zum Procedere einer solchen Prüfung liegen der Bundesregierung aber bisher keinerlei Informationen vor.

6. Welche neuen rechtlichen Mittel sollten den europäischen Behörden im Kampf gegen den Terrorismus „an die Hand“ gegeben werden, „um den Gebrauch von verschlüsselter elektronischer Kommunikation im Rahmen strafrechtlicher und administrativer Ermittlungen berücksichtigen zu können“, wie es der Bundesminister des Innern Thomas de Maizière mit seinem französischen Amtskollegen zuletzt an die Europäische Kommission übermittelte und kurz darauf mit dem EU-Kommissar Dimitris Avramopoulos besprach (Pressemitteilung BMI vom 21. Februar 2017, „EU-Kommissar Avramopoulos zu Gast im BMI“)?

Auf Grundlage der gemeinsamen Initiative der beiden Innenminister von Deutschland und Frankreich haben die jeweiligen Ministerien gemeinschaftlich Forderungen und mögliche Regelungsvorschläge erarbeitet und diese der Europäischen Kommission zur gemeinsamen Erörterung übermittelt.

Ziel ist es, geeignete Lösungen zu finden, um in technischer und juristischer Hinsicht der zunehmenden Verwendung von verschlüsselter Kommunikation durch kriminelle und terroristische Vereinigungen zu begegnen. Zugleich soll ein hohes Schutzniveau der Systeme gewährleistet werden, um die Verschlüsselungstechnologien für Benutzer und Wirtschaft nicht zu schwächen. Unter anderem wird gefordert, Verpflichtungen, wie sie bisher für Telekommunikationsdienste gelten, auch auf Telemediendienste auszuweiten, also allen Kommunikationsdienstleistern aufzuerlegen.

7. Worum handelt es sich beim Projekt „MedSec TP Net“ zur Schaffung eines Netzwerkes zwischen Sicherheitsakteuren im Mittelmeerraum, das im Rahmen des EU-Forschungsrahmenprogramms „Horizon 2020“ durchgeführt wird und an dem sich die Bundespolizei beteiligt?

Im Rahmen des EU-Sicherheitsforschungsprogramms wird auch die Bildung von Netzwerken von Sicherheitsakteuren gefördert. Unter der Bezeichnung „MedSec TP Net“ hat sich ein Konsortium um Fördermittel beworben, welches ein paneuropäisches Netzwerk zwischen Sicherheitsakteuren im Mittelmeerraum zur Verbesserung der Kommunikation und Koordination zwischen Endnutzern (EU und Nicht-EU Sicherheitsbehörden) und Anbietern von Sicherheitstechnologien begründen wollte.

Dieses Netzwerk sollte die Möglichkeiten zur Durchführung gemeinsamer Grenzschutzmissionen und der Bewältigung von Krisensituationen durch Informationsaustausch und Interoperabilität von Systemen und Methoden in der Mittelmeerregion verbessern. Nach Mitteilung des maßgeblich an der Bildung des Konsortiums beteiligten Unternehmens hat das Projekt im Ergebnis des Ausschreibungsverfahrens jedoch keine Förderung erhalten.

a) Welche weiteren Partner arbeiten mit welchen Beiträgen in dem Projekt mit?

Es findet keine Projektarbeit statt, da das Projekt zunächst nicht zustande gekommen ist.

b) Welche „Nicht-EU Sicherheitsbehörden“ welcher Länder sollten aus Sicht der Bundesregierung an der in Projekt „MedSec TP Net“ entwickelten „Kommunikation und Koordination zwischen Endnutzern“ teilnehmen?

Auf die Antwort zu Frage 7a wird verwiesen.

8. Worum handelt es sich nach Kenntnis der Bundesregierung bei dem EU-Forschungsprojekt „Maritime Integrated Surveillance Awareness“ (MARIS), das nach Kenntnis der Fragesteller dem „Kampf gegen die illegale Einwanderung, Menschenschmuggel, Terrorismus und Piraterie“ dienen soll, welche Methoden werden darin entwickelt, und wer nimmt daran teil?

Nach Kenntnis der Bundesregierung ist von Seiten der Europäischen Kommission im Bereich „Sichere Gesellschaften“ des Rahmenprogramms „Horizon 2020“ ein Projektvorschlag „MARISA – Maritime Integrated Surveillance Awareness“ zur Förderung ausgewählt, jedoch bisher nicht bewilligt worden. Aktuelle Informationen zu Verfahren und Inhalten liegen der Bundesregierung nicht vor.

9. Welche Daten welcher Informationssysteme werden in dem Projekt verarbeitet und kompatibel gemacht?

Auf die Antwort zu Frage 8 wird verwiesen.

10. Was ist der Bundesregierung darüber bekannt, inwiefern die Projekte „Decision Support Platform for Detecting Radicalisation and Over/Cover Terrorist Communications through the Internet“, „Real-Time Early Detection and Alert System for Online Terrorist Content based an SNA and Complex Event Processing“ und „DEtecting TErrorist ContentT and the InterneT“ mittlerweile im EU-Forschungsrahmenprogramm „Horizon 2020“ zur Förderung ausgewählt wurden (Bundestagsdrucksache 18/7794, Schriftliche Frage 13 des Abgeordneten Andrej Hunko), welches Ziel verfolgen die Projekte, und wer nimmt daran teil?

Nach Kenntnis der Bundesregierung sind die genannten Projektvorschläge im Rahmenprogramm „Horizon 2020“ nicht zur Förderung ausgewählt worden.

11. Was ist der Bundesregierung über Ziel, Inhalt und Teilnehmende eines im Rahmen des EU-Forschungsrahmenprogramms „Horizon 2020“ durchgeführten Projekts „Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings“ (LETS-CROWD) bekannt (http://gleft.de/1BZ)?

Nach Kenntnis der Bundesregierung ist von Seiten der KOM im Bereich „Sichere Gesellschaften“ des Rahmenprogramms „Horizon 2020“ ein Projektvorschlag „LETS-CROWD – Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings“ zur Förderung ausgewählt, jedoch bisher nicht bewilligt worden. Aktuelle Informationen zu Verfahren und Inhalten liegen der Bundesregierung nicht vor.

12. Worum handelt es sich bei dem ebenfalls im Rahmen des EU-Forschungsrahmenprogramms „Horizon 2020“ durchgeführten Projekts „Tools for the Investigation of TrANsactions In Underground Markets“ (TITANIUM) des Bundeskriminalamtes, welches Ziel wird darin verfolgt, und wer nimmt daran teil (Bundestagsdrucksache 18/10929, Frage 19 der Kleinen Anfrage der Fraktion DIE LINKE.)?

Ziel des Forschungsprojektes TITANIUM (Tools for the Investigation of TrANsactions In Underground Markets) ist die Entwicklung von Technologien und Werkzeugen zur Bekämpfung von Straftaten und terroristischen Aktivitäten, bei denen virtuelle Währungen und / oder Untergrundmärkte genutzt werden. Die Implementierung der Ergebnisse in die polizeiliche Arbeit wird durch die Ausarbeitung von Ausbildungskonzepten und Vermittlung in Fortbildungsveranstaltungen unterstützt.

Am Projekt beteiligt sind:

- Austrian Institute of Technology GmbH - Projektleitung
- Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
- Universität Innsbruck
- Karlsruher Institut für Technologie
- University College London
- Fundacion Centro de Tecnologias de Interaccion Visual y Comunicaciones Vicomtech
- Coblue Cybersecurity
- Dence GmbH
- Trilateral Research Ltd.
- Countercraft S.L.
- The International Criminal Police Organization
- National Bureau of Investigation (Finland)
- Österreichisches Bundesministerium für Inneres
- Spanisches Ministerio del Interior
- BKA.

Darüber hinaus beteiligen sich neun Polizeidienststellen aus dem Vereinigten Königreich, Zypern, Rumänien, den Niederlanden, Polen, Portugal, Schweden und der Schweiz sowie Europol und die Europäische Zentralbank am Projekt, indem sie Anforderungen einbringen und Entwicklungsergebnisse bewerten.

13. Welche Aufgaben werden vom Kriminaltechnischen Institut des Bundeskriminalamtes und von Interpol im EU-Forschungsprojekt „Speaker Identification Integrated Project“ (SiiP) übernommen (www.siip.eu)?

Das Kriminaltechnische Institut des BKA hat im SIIP-Projekt (Speaker Identification Integrated Project) primär eine beratende Funktion und wird Aufgaben bei der Validierung der Systemperformanz im Rahmen von Feldversuchen sowie im Bereich des Anwendertrainings übernehmen.

a) Welche Techniken und Verfahren der Sprachverarbeitung und forensischen Phonetik werden in SiiP beforscht?

Im Rahmen von SIIP werden keine Techniken und Verfahren der forensischen Phonetik erforscht, sondern Techniken und Verfahren der automatischen Sprecheridentifizierung.

b) Inwiefern sind auch Geheimdienste mittelbar oder unmittelbar an SiiP beteiligt?

An SIIP sind ausschließlich Polizeibehörden, Universitäten und kommerzielle Unternehmen beteiligt.

c) Was ist der Bundesregierung darüber bekannt, inwiefern die in dem Forschungsprojekt erlangten Erkenntnisse oder Ergebnisse über dort beteiligte Firmen auch Geheimdiensten zugänglich gemacht werden sollen?

Die Nachrichtendienste waren weder mittelbar noch unmittelbar an SIIP beteiligt.

d) Inwiefern werden beim Bundeskriminalamt mittlerweile Techniken zum sogenannten Textmining eingesetzt (Bundestagsdrucksache 17/14832, Antwort zu Frage 3 der Kleinen Anfrage der Fraktion DIE LINKE.)?

Im Kriminaltechnischen Institut werden keine Techniken zum forensischen Textmining eingesetzt. Die Technik soll im BKA künftig genutzt werden, um beispielsweise Verwaltungsinformationen (Gremien-, Besprechungsbeschlüsse u. ä.) mittels Volltextsuche strukturiert auf relevante Inhalte durchsuchen zu können. Dies soll nach derzeitigem Planungsstand mit kommerziellen Produkten, die zur Literaturverwaltung, Wissensverwaltung oder Aufgabenplanung geeignet sind, realisiert werden.

e) Welche „marktgängige[n] Produkte“ nutzt der Bundesnachrichtendienst zur Sprechererkennung oder für Zwecke des automatischen Stimmenvergleichs, und auf welche Weise integriert der Auslandsgeheimdienst diese „in eigene Prozesse“ (Bundestagsdrucksache 17/14832, Antwort zu Frage 6 der Kleinen Anfrage der Fraktion DIE LINKE.)?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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