Deutscher Bundestag **Drucksache 18/11578**

18. Wahlperiode 20.03.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Inge Höger, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/11362 –

Verfahren zur internationalen Herausgabe elektronischer Beweismittel

Vorbemerkung der Fragesteller

Aus Gründen der Geheimhaltung will das Bundesministerium des Innern nicht angeben, bei welchen US-Betreibern von „Cloud-Diensten“ deutsche Behörden im Zuge von Ermittlungen Direktanfragen für sogenannte elektronische Beweismittel stellen und in welchem Umfang diese Ersuchen beantwortet werden (Bundestagsdrucksache 18/10948, Netzpolitik vom 3. Februar 2017, „Ermittlung in der ‚Cloud‘: Innenministerium will keine Zahlen nennen“). Unklar bleibt, warum die Bundesregierung die Zahlen nicht öffentlich machen will, die Europäische Kommission aber derweil ähnliche Statistiken bekannt gibt (Ratsdok. 15072/1/16). Um an Daten im Ausland zu gelangen, gehen Behörden entweder den offiziellen Weg der internationalen Rechtshilfe oder klopfen direkt bei den Anbietern an. Die Bundesregierung wünscht sich reibungslosere Verfahren. Deshalb arbeite man laut der Bundesregierung gemeinsam mit der Europäischen Union und den jeweiligen Partnerstaaten an verbesserten Prozessen, um schneller zu Ergebnissen zu kommen und „die Abläufe im Rahmen der Rechtshilfe zu beschleunigen und zu optimieren“ (Bundestagsdrucksache 18/10948). Bei der Europäischen Kommission habe die Bundesregierung einen Regelungsvorschlag eingebracht, um die „Europäische Ermittlungsanordnung in Strafsachen (EEA) um eine Vorschrift zur grenzüberschreitenden Sicherung elektronischer Daten ohne technische Hilfe zu ergänzen“. Diese Vorschrift könnte sich an das in der Europäischen Ermittlungsanordnung verankerte, „für die Überwachung von Telekommunikationsverkehr ohne technische Hilfe vorgesehene Modell einer Notifikation anlehnen“. Konkrete Vorschläge der Kommission seien im Sommer 2017 zu erwarten. Für den Zugriff auf außerhalb der EU liegende Daten sei der Abschluss einer entsprechenden internationalen Vereinbarung notwendig. Ob es dazu kommt, sei es durch einen bilateralen Vertrag zwischen Deutschland und den USA oder eine gesamteuropäische Lösung, bleibt derzeit offen. Zur Debatte steht auch eine Ausweitung der Cybercrime-Konvention des Europarates. Der dort zuständige Ausschuss hat hierzu bereits mit Beratungen begonnen. Die Entwicklung technischer Spezifikationen für Schnittstellen zur Herausgabe elektronischer Beweismittel könnte beim European Telecom Standards Institute (ETSI) erfolgen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 16. März 2017 übermittelt.

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

1. Auf welche Weise ist der Ausschuss zur Cybercrime-Konvention (Cybercrime Convention Committee, T-CY) damit befasst, die Cybercrime-Kovention durch ein Zusatzprotokoll mit Regelungen zur Erleichterung der Rechtshilfe zu ergänzen (Bundestagsdrucksache 18/10948, Antwort zu Frage 14), und wann soll ein Vorschlag dazu vorliegen?

Der T-CY kam bei der vergangenen Plenarsitzung im November 2016 grundsätzlich überein, dass Bedarf für ein (weiteres) Zusatzprotokoll zur Konvention besteht. Die vom T-CY eingesetzte Cloud Evidence Group (CEG) wurde aufgefordert, im Frühjahr 2017 einen Mandatsentwurf für das Ausarbeitungsverfahren und zu den möglichen Inhalten eines solchen Zusatzprotokolls vorzulegen. Nachdem die CEG den Mandatsentwurf im März an die Mitglieder des T-CY übermittelt und ihnen Gelegenheit zur Stellungnahme gegeben hat, soll dieser bei der kommenden Plenarsitzung im Juni 2017 angenommen werden. Der Mandatsentwurf sieht vor, dass der T-CY die Arbeiten an dem Entwurf für das Zusatzprotokoll bis Dezember 2019 abschließt.

2. Welche Hindernisse bzw. Defizite sieht die Bundesregierung hinsichtlich der Einrichtung und Nutzung von Schnittstellen zur internationalen Herausgabe elektronischer Beweismittel bei ihren hierfür zuständigen Behörden?

Schnittstellen zur internationalen Herausgabe elektronischer Beweismittel müssen den rechtlichen und technischen Anforderungen genügen. Bei dem jetzigen Stand der Angelegenheit können keine weiteren konkreten Angaben gemacht werden.

3. Was ist der Bundesregierung darüber bekannt, auf welche Weise das ETSI mit der Entwicklung technischer Spezifikationen für Schnittstellen zur Herausgabe elektronischer Beweismittel befasst ist?

   a) Inwiefern hat das ETSI hierzu bereits Vorschläge vorgelegt, und welchen Tenor haben diese?

   b) Welche einzelnen Daten bzw. Datenströme sind von diesen Spezifikationen erfasst?

   c) Inwiefern enthalten die Vorschläge auch die Möglichkeit von Direktanfragen bei den betreffenden Internetanbietern?

   d) Welche Behörden und Firmen waren an der Erstellung der Spezifikationen beteiligt, und welche Beiträge haben Bundesbehörden hierfür erbracht?

   e) Wann, wo und von wem sollen die Schnittstellen getestet werden?

Die Fragen 3 bis 3e werden zusammen beantwortet. Die Antwort der Bundesregierung zu Frage 3 würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch außerhalb der Bundesrepublik Deutschland – zugänglich machen. Dies wäre für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage 3 aus Geheimhaltungsgründen nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden.

Im konkreten Fall kann den Sicherheitsinteressen der Bundesregierung jedoch durch Übermittlung einer eingestuften Antwort entsprochen werden. Die Antwort auf diese Frage wird daher als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft.*

4. Was ist der Bundesregierung über die weiteren Diskussionen zur Einrichtung eines Internetportals bekannt, mit dem sich in einem ersten Schritt die Ermittlungsbehörden und Staatsanwaltschaften in der Europäischen Union vernetzen (Bundestagsdrucksache 18/10948, Antwort zu Frage 18)?

Die Arbeiten der Europäischen Kommission an der Einrichtung des Internetportals befinden sich nach Kenntnis der Bundesregierung noch in einem verhältnismäßig frühen Stadium und befassen sich derzeit mit grundsätzlichen Fragen wie z. B. der möglichen (zentralen oder dezentralen) Struktur des Portals. Konkrete Vorschläge der Kommission zur Einrichtung des Internetportals liegen noch nicht vor.

5. Wann könnte der Prototyp für ein solches Portal betriebsbereit sein?

Der für die Einrichtung des Systems zu veranschlagende Zeitrahmen variiert nach vorläufiger Einschätzung der Europäischen Kommission zwischen 18 und 30 Monaten.

6. Was ist der Bundesregierung mittlerweile darüber bekannt, für welche Maßnahmen die Generaldirektion Justiz und Verbraucherschutz der Europäischen Kommission 1 Mio. Euro bereitstellt, um die rechtlichen Möglichkeiten der Rechtshilfe beziehungsweise Direktanfragen zu analysieren, bzw. wann die Ausschreibung, bei der Projekte zur Erlangung elektronischer Beweismittel vorrangig berücksichtigt werden, beendet ist (Bundestagsdrucksache 18/10948, Antwort zu den Fragen 11 und 12)?

Auf die Antwort der Bundesregierung zu den Fragen 11 und 12 der Kleinen Anfrage auf Bundestagsdrucksache 18/10948 wird verwiesen. Die dort benannte Ausschreibung der Europäischen Kommission kann auch Projekte zur Erlangung elektronischer Beweismittel umfassen. Zudem ist im Zwischenbericht der Europäischen Kommission (Ratsdok. 15072/1/16) zur Umsetzung der Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ auf Seite 17 ein Budget von 1 Mio. Euro erwähnt, das gezielten Maßnahmen im Bereich der EU-US Kooperation betreffend elektronische Beweismittel dienen soll. In welchem Verhältnis dies zur erwähnten Ausschreibung steht, ist der Bundesregierung gegenwärtig nicht bekannt.

7. Was ist der Bundesregierung darüber bekannt, inwiefern im Rahmen des EU-Internet-Forums bzw. dessen Roundtable-Veranstaltungen weitere private Sachverständige einbezogen werden?

   a) Um welche Veranstaltungen bzw. Akteure handelt es sich dabei?

   b) Welche Themen wurden mit den Sachverständigen erörtert?

Die Fragen 7 bis 7b werden gemeinsam beantwortet.

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

Das sog. EU-Internet Forum verfolgt das Ziel, die EU-Mitgliedstaaten in einen Dialog mit Vertretern führender Internet-Diensteanbieter hinsichtlich der Reduzierung von terroristischer Online-Propaganda zu bringen. Die Einladungen erfolgen durch die veranstaltende Europäische Kommission. Einziger externer Vortragender auf der letzten Sitzung am 8. Dezember 2016 war das von der EU finanzierte akademische Wissenschaftsnetzwerk „VOX-Pol Network of Excellence“. Private Sachverständige wurden bislang nicht einbezogen.

8. Was ist der Bundesregierung darüber bekannt, auf welche Weise die Frage des Zugangs von Sicherheitsbehörden zu verschlüsselten Inhalten auf EU-Ebene weiter behandelt wird und welche Arbeitsgruppen hierzu welche Treffen, Workshops oder Konferenzen planen?

Der Bundesregierung ist bekannt, dass die Europäische Kommission aktuell Überlegungen anstellt, wie dem zunehmenden Aufkommen von verschlüsselten Inhalten in Strafverfahren Rechnung getragen werden kann. Das Thema „Encryption“ ist nach aktuellem Stand auch für die Tagesordnung des JI-Rates (Justiz-Teil) Ende März 2017 vorgesehen. Darüber hinaus geht die Bundesregierung davon aus, dass das Sujet auch in künftigen Sitzungen der EU-Arbeitsgruppe „Horizontal Working Party on Cyber Issues“ (HWP) thematisiert wird.

9. Welche Bundesbehörden waren oder sind an dem EU-Forschungsprojekt „Evidence“ zur internationalen Herausgabe elektronischer Beweismittel beteiligt, und welches Ziel wird dort verfolgt?

   a) Mit welchem Ziel beteiligt sich Interpol an dem Forschungsprojekt, und welche Beiträge erbringt die Polizeiorganisation dort?

   b) Welcher Fahrplan zur Umsetzung der Ergebnisse des Projekts ist der Bundesregierung bekannt?

Die Fragen 9 bis 9b werden gemeinsam beantwortet. Die Bundesregierung ist an dem Projekt nicht beteiligt; ihr liegen derzeit keine weiteren Erkenntnisse im Sinne der Fragestellung vor.

10. Inwiefern ist der Bundesregierung über die Angaben auf Bundestagsdrucksachen 18/11041 und 18/10591 bekannt, ob und wann das neue „Netzwerk der Justizbehörden und Experten im Bereich Cyberkriminalität“ (EJCN) ein erstes Arbeitsprogramm vorlegen will?

Auf die Antworten der Bundesregierung zu den Fragen 16 und 17 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11263 vom 8. Dezember 2016 wird verwiesen. Nach Kenntnis der Bundesregierung hat seit dem Treffen vom 24. November 2016 kein weiteres Treffen des EJCN stattgefunden.

11. Was ist der Bundesregierung über Angehörige eines EU-Netzwerkes „European Network of law enforcement specialists on Carrier-Grade Network Address Translation“ bekannt, und welche Treffen der Gruppe haben bereits stattgefunden (Pressemitteilung Europol vom 2. Februar 2017)?

Am 31. Januar 2017 hat das erste Treffen der Expertengruppe (EC3) stattgefunden. Daran haben Vertreter des Bundeskriminalamtes teilgenommen.

12. Welche Haltung vertritt die Bundesregierung zur Frage, ob sich auch das EU-Internet-Forum mit dem Problem der Carrier-Grade Network Address Translation bzw. sich daraus ergebenden Defiziten für Sicherheitsbehörden hinsichtlich auf Vorrat gespeicherter Telekommunikationsdaten befassen sollte?

Hinsichtlich der Zielsetzung des sog. EU Internet Forums wird auf die Antwort zu Frage 7 verwiesen. Die in der Fragestellung genannten Themenfelder enthalten keine Berührungspunkte zu der bisherigen Zielsetzung und bieten sich daher nach Ansicht der Bundesregierung nicht für eine Erörterung in dem Forum an.

13. Welche weiteren Erläuterungen kann die Bundesregierung zu ihrem bei der Konferenz „Crossing Borders: Jurisdiction in Cyberspace“ vom 6. bis 8. März 2016 in Amsterdam vorgelegten Vorschlag für eine „Notifikationslösung“ machen (Ratsdok. 15072/16, Bundestagsdrucksache 18/10948, Antwort zu Frage 2)?

Zu der von der niederländischen Ratspräsidentschaft vom 6. bis 8. März 2016 in Amsterdam ausgerichteten Konferenz „Crossing Borders: Jurisdiction in Cyberspace“ wurde von der Bundesregierung ein vorbereitender Beitrag vorgelegt. Darin wurde angeregt, die Möglichkeit zu prüfen, für die direkte grenzüberschreitende Sicherung gespeicherter Daten auf der Ebene der Europäischen Union ein Kooperationsinstrument nach dem Vorbild von Artikel 31 der Richtlinie 2014/41/EU vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (RL EEA) zu schaffen. Ähnlich wie in den in Artikel 31 RL EEA geregelten Fällen der direkten grenzüberschreitenden Telekommunikationsüberwachung erscheint es auch in Fällen der grenzüberschreitenden Sicherung gespeicherter Daten überlegenswert, zwischen den Mitgliedstaaten der Europäischen Union ein Verfahren einzuführen, bei dem der ermittelnde Mitgliedstaat den von der Maßnahme betroffenen Mitgliedstaat nachträglich von der Maßnahme unterrichtet und der unterrichtete Mitgliedstaat sodann widersprechen kann, falls eine entsprechende Maßnahme nach seinem eigenen Recht nicht zulässig wäre.

a) Wo wurde der Vorschlag weiter beraten oder diskutiert?

Der o. g. vorbereitende Beitrag war ausschließlich für die Konferenz „Crossing Borders: Jurisdiction in Cyberspace“ konzipiert. Die zugrundeliegende Idee einer Notifikationslösung für die grenzüberschreitende Sicherung gespeicherter Daten war in der Folge auch Gegenstand eines Regelungsansatzes, den die Bundesregierung als Diskussionsbeitrag in dem von der Europäischen Kommission in Umsetzung der Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ vom 9. Juni 2016 (Ratsdok. 10007/16) durchgeführten Konsultationsprozess mit den Mitgliedstaaten vorgestellt hat.

b) Welche Haltungen vertreten die übrigen EU-Mitgliedstaaten zu dem Vorschlag, die Richtlinie 2014/41/EU vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (RL EEA) um eine Vorschrift zur grenzüberschreitenden Sicherung elektronischer Daten ohne technische Hilfe zu ergänzen?

Bisher hat dazu lediglich ein fachlicher Austausch stattgefunden. Die anderen Mitgliedstaaten haben sich zu dem Regelungsvorschlag noch nicht positioniert.

c) Wann im Sommer 2017 will die Europäische Kommission ihre Prüfung zu derzeit möglichen „Formen des unmittelbaren Zugangs zu elektronischen Beweismitteln“ beendet haben?

Die Europäische Kommission hat in ihrem Zwischenbericht vom 7. Dezember 2016 (Ratsdok. 15072/1/16) angekündigt, zur Sitzung des JI-Rates im Juni 2017 Optionen vorzuschlagen, aufgrund derer im weiteren Verlauf konkrete Lösungen ausgearbeitet werden können.

d) Welche weiteren Ausführungen zur RL EEA sowie darüber hinaus enthält der „Regelungsvorschlag“, den die Bundesregierung der Europäischen Kommission hierzu als „Diskussionsbeitrag“ übermittelt hat?

Auf die Antworten zu den Fragen 13 und 13a wird verwiesen. Der Regelungsansatz enthält keine weiteren Ausführungen zur RL EEA.

e) Welche weiteren Problemstellungen wurden auf der Konferenz in den Workshops A „Creating effective MLA processes“ und Workshop C „Crime from nowhere; legal challenges for unknown locations“ behandelt, und welche Lösungen wurden skizziert?

Die Workshops A „Creating effective MLA processes“ und C „Crime from nowhere; legal challenges for unknown locations“ befassten sich mit Herausforderungen für die internationale Kooperation in Strafsachen, die sich mit Blick auf die Gewinnung elektronischer Beweismittel ergeben. Unter anderem besteht hier wegen der Flüchtigkeit von elektronischen Daten ein erhöhtes Risiko des Beweismittelverlustes. Diskutiert wurde daher neben dem in den Antworten zu den Fragen 13 und 13a beschriebenen Regelungsansatz auch, welche Möglichkeiten zur Vereinfachung und Beschleunigung von Rechtshilfeverfahren denkbar sind. Darüber hinaus lässt sich der physische Speicherort von elektronischen Daten in bestimmten Fällen wie z. B. beim Cloud-Computing nur schwer oder überhaupt nicht bestimmen. Deshalb wurde diskutiert, ob und wie in Anbetracht dieses Umstands die Rechtshilfe weiterzuentwickeln ist.

14. Was ist der Bundesregierung darüber bekannt, in welchem Maße Sicherheitsbehörden aus EU-Mitgliedstaaten zur Herausgabe von Telekommunikationsdaten selbst das Internet oder die Telekommunikation in anderen Ländern (etwa mit Trojanern) überwachen?

Der Bundesregierung liegen keine entsprechenden Erkenntnisse vor.

a) Hat es nach Kenntnis der Bundesregierung bereits Fälle gegeben, in denen deutsche Sicherheitsbehörden per „Fernzugriff“ in der Cloud zu ermitteln haben, auch wenn der physische Ort der Server unbekannt war (Bundestagsdrucksache 18/10948, Antwort zu Frage 16)?

Die Bundesregierung kann dazu keine abschließende Auskunft erteilen, weil die Strafverfolgung grundsätzlich in der Zuständigkeit der Länder liegt. Darüber hinaus werden Fälle, in denen deutsche Strafverfolgungsbehörden „in der Cloud ermittelt“ haben, um Beweismittel zu erlangen, von der Bundesregierung nicht statistisch erfasst.

b) Welche nationalen Befugnisnormen und anwendbaren völkerrechtlichen Verträge lagen dabei bezüglich der „Fernzugriffe“ von Bundesbehörden zugrunde?

Als Rechtsgrundlage kann § 110 Absatz 3 der Strafprozeßordnung (StPO), ggf. i. V. m. Artikel 32 der Cybercrime-Konvention dienen, wobei deren Voraussetzungen und Reichweite zu beachten sind, insbesondere auch in Fällen nicht genau bestimmbarer Datenspeicherorte.

15. Welche weiteren Details kann die Bundesregierung zu den im Strategie- und Forschungszentrum Telekommunikation (SFZ TK) durchgeführten Einzelprojekten INTLI („Internationale Zusammenarbeit in der Telekommunikationsüberwachung“) und SMART („Informationstechnische Überwachung mobiler Endgeräte“) mitteilen (Plenarprotokoll 18/214, Antwort auf die Mündliche Frage 8 des Abgeordneten Andrej Hunko)?

a) Welches Ziel wird mit den Projekten verfolgt, und wann sollen Ergebnisse bzw. Prototypen vorliegen?

b) Wer führt die Projekte an, und wer nimmt (auch beratend) daran teil?

Die Fragen 15 bis 15b werden gemeinsam beantwortet.

Die Antwort zu Frage 15 einschließlich der Fragen 15a und 15b würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch außerhalb der Bundesrepublik Deutschland – zugänglich machen.

Dies wäre für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage 3 aus Geheimhaltungsgründen nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden.

Im konkreten Fall kann den Sicherheitsinteressen der Bundesregierung jedoch durch Übermittlung einer eingestuften Antwort entsprochen werden. Die Antwort auf diese Frage wird daher als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft.*

c) In welchen Bundesländern darf die Telekommunikation von Gefährdern nach Kenntnis der Bundesregierung überwacht werden, in welchen ist die Quellen-Telekommunikationsüberwachung und in welchen die Online-Durchsuchung erlaubt?

Der Bundesregierung liegt über die öffentlich zugänglichen gesetzlichen Regelungen hinaus keine verbindliche Übersicht zur Praxis in den Bundesländern vor.

16. Welche Softwarekomponenten welcher Hersteller werden für die Prognosesysteme des Bundeskriminalamtes RADAR-iTE („regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus“) und RISKANT genutzt (http://gleft.de/1BC)?

Bei der Durchführung einer Risikobewertung im Rahmen von RADAR-iTE kommen die beiden Standard-Komponenten „Excel“ sowie „Word“ des Microsoft-Office-Systems zum Einsatz. Es ist keine spezielle Anwendung für diese Zwecke

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

entwickelt worden. Bei RISKANT handelt es sich um ein derzeit noch in der Planung befindliches Projekt. Über Softwarekomponenten, die hierbei ggf. Verwendung finden werden, sind daher zum jetzigen Planungsstand noch keine Angaben möglich.

17. Auf welche Weise erhielten und erhalten die nach § 100 der Strafprozessordnung zum Abhören von Telekommunikation berechtigten Bundesbehörden herausverlangte Daten von den Handy-Providern (bitte darstellen, bis zu welchem Jahr Datenträger wie Diskette, CD, USB-Stick und/oder Fax sowie technische Schnittstellen genutzt wurden)?

Die Regelungen des § 100 StPO umfassen das Verfahren der Postbeschlagnahme. Bei der nachfolgenden Beantwortung der Frage 17 wird daher davon ausgegangen, dass von Seiten der Fragesteller die Regelungen zur Telekommunikationsüberwachung gemäß den §§ 100a ff. StPO gemeint sind.

Die technische Durchführung der Telekommunikationsüberwachung richtet sich nach der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV). Die Übermittlung der Überwachungskopie richtet sich nach § 9 TKÜV. Die gemäß TKÜV zur Herausgabe von Daten verpflichteten Anbieter von Telekommunikationsdiensten übersenden die angeforderten Daten providerabhängig auf unterschiedliche Art und Weise an die berechtigten Stellen. Abhängig von Größe und Umfang der Daten kommen verschiedene Datenträger oder Übermittlungswege in Betracht. Eine statistische Erfassung der jeweiligen Übermittlungswege liegt hierzu nicht vor.

18. Welche weiteren Details kann die Bundesregierung zu dem deutschen Projektvorschlag zur Verbesserung des DNA-Datentauschs im Prüm-Verfahren mitteilen (http://gleft.de/1Bq)?

Die Projektvorschläge des Bundeskriminalamtes „DNA onEU“ im Dezember 2014 bzw. „DNA fEUsion“ im Dezember 2015 befassen sich mit der Optimierung und Verbesserung des IT-Wirkbetriebs des Austausches der DNA-Profile in den angeschlossenen EU-Mitgliedstaaten. Gemäß dem völkerrechtlichen Vertrag von Prüm von 2006/2007 ist der Datenaustausch in den Bereichen DNA-, Fingerabdrücke- und Kfz-Daten zwischen den Polizei/Justiz-Behörden der vertraglichen EU-Staaten umgesetzt und im Wirkbetrieb implementiert. Der Vertrag von Prüm wurde in 2008 in den EU-Rahmen integriert. Alle EU-Mitgliedstaaten sollen innerhalb einer Frist an diesem Verfahren teilnehmen.

Hinsichtlich der dezentralen Datenbestände und heterogenen Kommunikationssysteme in den angeschlossenen EU-Mitgliedstaaten dienen die DE-Projektvorschläge überwiegend zur Erhöhung der Produktivität, Effektivität und Performanz in der IT-Umgebung aller angeschlossenen EU-Staaten.

a) Welche Hard- und Software sollte in dem Vorhaben genutzt oder entwickelt werden?

Im Rahmen dieses Vorhabens sollen keine neuen Hardwarekomponenten und keine neue Systemsoftware entwickelt oder genutzt werden. Lediglich werden die existierenden Applikationen verbessert und optimiert. Des Weiteren wird ein einheitlicher Satz von Schulungsunterlagen in den Bereichen Polizeiliche Fachlichkeit, Forensik und IT vom Projektteam entwickelt, in den EU-Staaten harmonisiert und als Schulungsmodule im Rahmen des CEPOL-Programms eingesetzt.

b) Inwiefern und mit welchen Teilnehmenden wurde oder wird das Projekt umgesetzt und weiterverfolgt?

Im Vorfeld des Projektvorschlages konnten die vier EU-Staaten (Frankreich, Polen, Tschechische Republik und Slowenien) als offizielle Partnerstaaten gewonnen werden. Falls das Projekt von der EU-Kommission genehmigt wird, wird dieses Projekt unter Federführung des Bundeskriminalamtes in Kooperation mit den vier Partnerstaaten durchgeführt. Die Etappenergebnisse werden im Rahmen der offiziellen Sitzungen der EU-Arbeitsgruppen DAPIX vorgestellt. In Bezug auf neue Anforderungen bzw. Wünsche aller EU-Staaten sind die Umsetzungsprozeduren des Projektes im Lauf der Projektdurchführung anzupassen, um maximale Nutzbarkeit der Produkte in allen EU-Staaten bieten zu können.

19. Von welchem Hersteller hat das Bundeskriminalamt im zweiten Halbjahr 2016 die Software „Examiner“ für automatisierte Lichtbildvergleiche beschafft (Bundestagsdrucksache 18/11041, Antwort zu Frage 7)?

Die vom BKA beschaffte Software „Examiner“ stammt von der Firma Cognitec Systems GmbH aus Dresden.

a) Wann und im Rahmen welcher Verfahren soll die Software genutzt werden?

Die vorgenannte Software „Examiner“ wird im Rahmen der Zentralstellenaufgabe des Bundeskriminalamts eingesetzt und dient im Bereich der religiös motivierten Kriminalität (Zentrale Phänomenauswertung) der Gewinnung von Ermittlungsansätzen in Form von Personenidentifizierungen anhand von automatisierten Lichtbildvergleichen. Die Aufnahme eines Probewirkbetriebs steht in Kürze bevor.

b) Unter welchen Voraussetzungen kann die Software auch Standbilder aus Bewegtbildern verarbeiten?

Das Gesichtserkennungssystem ermöglicht derzeit keine automatische Verarbeitung von Bewegtbildern im Sinne eines Video-Scans und den automatisierten Abgleich von darin enthaltenen Gesichtern/Porträts. In den automatisierten Lichtbildvergleich mittels der „Examiner“- Software können jedoch zuvor manuell erzeugte Standbilder mit Gesichtern/Porträts aus Bewegbildern einbezogen werden. Ergänzend wird auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11041 vom 30. Januar 2017 verwiesen.

c) Unter welchen Voraussetzungen könnte die Software außer dem zentralen und verbundfähigen Lichtbildbestand von INPOL-Zentral sowie dem Lichtbildbestand der Abteilung Staatsschutz auch Gesichtsbilder des Schengener Informationssystems verarbeiten?

Eine Nutzung der Software für den Lichtbildbestand im Schengener Informationssystem für Zwecke der automatisierten Gesichtserkennung ist derzeit fachlich nicht geplant und kann daher nicht bewertet werden.

20. Welche Bundesministerien und Behörden nehmen nach Kenntnis der Bundesregierung am „EU-US-Cyber-Dialog“ teil, der Ende 2017 wieder physisch zusammenkommen soll (Bundestagsdrucksache 18/10948, Antwort zu Frage 20)?

Der EU-US-Cyberdialog wird vom Europäischen Auswärtigen Dienst (EAD) und dem US Department of State organisiert und umfasst in erster Linie Vertreter des EAD, der Europäischen Kommission und verschiedener US-Behörden. Vertreter der EU-Mitgliedstaaten hatten beim letzten EU-US-Cyberdialog am 16. Dezember 2016 in Brüssel die Möglichkeit, als Beobachter teilzunehmen. Konkrete Teilnahmeplanungen auf Seiten der Bundesregierung für den EU-US Cyberdialog 2017 existieren zum jetzigen Zeitpunkt noch nicht.

21. Was ist der Bundesregierung über Ziele, Teilnehmende und Zeitpunkt bevorstehender Übungen der EU-Mitgliedstaaten zum Umgang mit einem Cyberangriff bekannt?

Im Rahmen der Übungsaktivitäten von ENISA sind verschiedene Übungen der EU-Mitgliedstaaten im Umgang mit einem Cyberangriff in Vorbereitung. Hierzu zählen dedizierte Übungen zu Verfahren der Abstimmung und des Informationsaustauschs (sog. SOP-Übungen, SOP = Standard Operating Procedure) sowie die EU-weite Übung Cyber Europe 2018 mit dem Ziel der Verbesserung der Zusammenarbeit zwischen den EU-Mitgliedstaaten (CSIRT-Ebene) bei der Bewältigung von länderübergreifenden IT-Sicherheitsvorfällen einschl. Cyberangriffen. Details zu Teilnehmern und Zeitpunkten liegen der Bundesregierung nicht vor.

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