Deutscher Bundestag **Drucksache 19/26112**

19. Wahlperiode 25.01.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Michel Brandt, Sevim Dağdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/25264 –

EU-Maßnahmen gegen Verschlüsselung unter deutscher Beteiligung

Vorbemerkung der Fragesteller

Als „Co-Aktionsleiter“ nehmen das Bundeskriminalamt (BKA), das Bayerische Landeskriminalamt und Europol auf Ebene der Europäischen Union mindestens seit 2015 an einer „European Expert Group on Cybercrime“ teil, die unter anderem Anonymisierungsverfahren und Verschlüsselungen behandelt (Antwort zu Frage 28 auf Bundestagsdrucksache 18/4193).

Auch die Gruppe „Freunde der Präsidentschaft zu Cyber“ (FoP Cyber) befasst sich mit Verschlüsselung und will für öffentliches Bewusstsein zum Thema sorgen, Handlungsempfehlungen geben und die Kommission mit „praktischen Beiträgen“ zu Gesetzgebungsvorschlägen unterstützen (Ratsdokument 14079/15).

Mit Unterstützung der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) wird 2016 ein Europäisches Justizielles Netzwerk für Cyberkriminalität (EJCN) eingerichtet (Ratsdokument 8482/17), zu dessen zwei Kernaufgaben die „Bewältigung der Herausforderungen von Verschlüsselung“ gehört, zuständig ist hierfür eine „Beobachtungsstelle für Verschlüsselung“.

Nach der Behandlung im Innen- und Justizrat startet die Kommission 2016 einen „Reflektionsprozess“ zur Rolle der Verschlüsselung in strafrechtlichen Ermittlungen (Ratsdokument 6890/17). Im Mai 2017 findet auf Einladung des Europol-Zentrums zur Bekämpfung der Cyberkriminalität (EC3) der erste „Expertenworkshop“ zu Verschlüsselung statt, das Bundeskriminalamt war dort mit Personal verschiedener Abteilungen vertreten (Antwort auf die Schriftliche Frage 13 der Abgeordneten Inge Höger auf Bundestagsdrucksache 18/12703). Im Ergebnis wurde beschlossen, statistische Informationen zu Herausforderungen von Verschlüsselung zu erheben und Fallstudien zur Verbreitung von Verschlüsselungstechniken zu beauftragen. Diskutiert wurde auch die „zentrale Bündelung“ technischer Kompetenzen und „Dienstleistungen“ bei Europol.

Damals hatte auch die EU-Kommission einen „Expertenprozesses zur Verschlüsselung“ eingerichtet (https://www.consilium.europa.eu/de/meetings/jha/2017/06/08-09), in ihrem „11. Fortschrittsbericht zur Sicherheitsunion“ (COM(2017) 608 final) kündigt sie einen Sechs-Punkte-Plan mit rechtlichen

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 25. Januar 2021 übermittelt.

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

und technischen Maßnahmen „zur Verbesserung der Entschlüsselungsfähigkeiten“ an. Die Justiz- und Innenminister fordern die Kommission anschließend „eindringlich“ auf, „der Frage weiter nachzugehen“ (https://www.consilium.europa.eu/de/meetings/jha/2017/12/07-08).

Anfang 2018 findet bei Europol in Den Haag ein weiterer Workshop zu Verschlüsselung statt, an dem das deutsche Bundeskriminalamt teilnimmt (Antwort auf die Schriftliche Frage 19 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/695).

In einem „Arbeitspapier“ an den Rat schlägt die Kommission vor, dass Europol eine Spionagesoftware zum Eindringen in Endgeräte der digitalen Kommunikation (Trojaner) entwickeln („[…] lawful access to relevant data in the context of criminal investigations before the data becomes encrypted“, Ratsdokument WK 12742/2018) und den Behörden der Mitgliedstaaten als Dienstleistung zur Verfügung stellen soll. Die technische „Lösung“ zum Eindringen in fremde Rechnersysteme soll in einer nichtöffentlichen Ausschreibung beschafft werden. Europol erhält weitere 5 Mio. Euro zum Aufbau einer „Entschlüsselungsplattform“ für Datenträger (Ratsdokument 5661/18). Für Brute-Force-Attacken nutzt Europol die Software „Hashcat“ und Supercomputer der Europäischen Union (Europol 2019 Consolidated Annual Activity Report).

2020 wird eine vom BKA zunächst als „Expertengruppe 5G“ eingerichtete europaweite „Ständige Gruppe der Leiter der Abhörabteilungen“ verstetigt und unter anderem auf verschlüsselte Kommunikation ausgeweitet (Ratsdokument 11517/20).

Am 18. September 2020 kündigt die Bundesregierung an, im Rahmen ihrer EU-Ratspräsidentschaft eine Erklärung zur Aushebelung verschlüsselter Kommunikation im Internet verabschieden zu wollen (Ratsdokument 10728/20). Nach verschiedenen Änderungen wird diese „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ am 25. November 2020 im Ausschuss der Ständigen Vertreter gebilligt (Ratsdokument 13245/20). Ebenfalls akkordiert werden die Schlussfolgerungen zur inneren Sicherheit und zu einer europäischen Polizeipartnerschaft mit Ausführungen zu Verschlüsselung, in denen legislative Maßnahmen gefordert werden.

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt, soweit parlamentarische Anfragen jedoch Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen eine Beantwortung sämtlicher Fragen in offener Form nur teilweise erfolgen kann.

Im Einzelnen:

Die Antwort zu Frage 9 ist in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft.* Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Behörden des Bundes stehen. Die Fragen betreffen zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten, ermittlungstaktischen Verfahrensweisen und Aktivitäten. Aus dem Bekanntwerden der Antworten könnten Rückschlüsse auf Vorgehensweise, Fähigkeiten und Methoden der Sicherheitsbehörden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb ist ein Teil der Antwort zu der genannten Frage gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (VS-Anweisung – VSA) in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft und wird als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Die Beantwortung der Frage 1 berührt in besonders hohem Maße das Staatswohl. Nach sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass auch das geringfügige Risiko ihrer Offenlegung nicht getragen werden kann und deshalb die Frage hinsichtlich der Sicherheitsbehörden des Bundes auch nicht in eingestufter Form beantwortet werden kann.

Das verfassungsmäßig verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch schutzwürdige Interessen von Verfassungsrang begrenzt, wozu auch und insbesondere Staatswohlerwägungen zählen.

Eine Bekanntgabe der angefragten Informationen und Offenlegung der Einzelheiten zu Überlegungen, Verfahren und möglichen Sachständen zu Forschungsvorhaben im Zusammenhang mit Maßnahmen und dem Umgang mit Verschlüsselung, insbesondere mit Ende-zu-Ende-verschlüsselten Daten, würde die Vorgehensweisen, taktischen Arbeitsabläufe und damit mittelbar auch sowohl auf die derzeitige als auch die geplante technische Ausstattung zur Gefahrenabwehr oder zur Verhinderung und Aufklärung von Straftaten offenlegen oder Rückschlüsse darauf ermöglichen. Dies würde die polizeiliche und nachrichtendienstliche Arbeitsfähigkeit und Aufgabenerfüllung der Strafverfolgungsbehörden sowie der Nachrichtendienste gefährden, weil Täter oder potentielle Zielpersonen ihr Verhalten anpassen und künftige Maßnahmen dadurch erschweren oder gar vereiteln könnten.

Dies ist jedoch nicht hinnehmbar, da die Gewinnung von Informationen durch eine IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr notwendig ist und für die Aufgabenerfüllung dieser Behörden und damit für die Sicherheit der Bundesrepublik Deutschland, insbesondere bei der Bekämpfung des Terrorismus und der politisch motivierten sowie der organisierten Kriminalität unerlässlich ist. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Eine Preisgabe dieser sensiblen Informationen würde sich auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich, wie auch auf die Durchsetzung des Strafverfolgungsanspruchs und die nachrichtendienstliche Informationsbeschaffung, außerordentlich nachteilig auswirken, womit letztlich der gesetzliche Auftrag der Sicherheitsbehörden des Bundes – verankert im Grundgesetz (Artikel 73 Nummer 10 GG, Artikel 87 GG) und im Bundeskriminalamtgesetz (BKAG), im Bundespolizeigesetz (BPolG), im Zollfahndungsdienstgesetz (ZFdG), Geldwäschegesetz (GwG), Unionszollkodex (UZK) sowie in § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG), § 3 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG), § 1 Absatz 1 und § 14 Absatz 1 des Gesetzes über den Militärischen Abschirmdienst (MADG) – nicht mehr sachgerecht erfüllt werden könnte.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Informationen sowohl für die Aufgabenerfüllung der Nachrichtendienste des Bundes als auch der Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben nicht ausreichend Rechnung tra-

* Das Bundesministerium des Innern, für Bau und Heimat 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.

gen, 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 der Sicherheitsbehörden des Bundes in einem durch den Bezug auf bestimmte Produkte derartigen Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen 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 überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

1. Welche eigenen Überlegungen oder Forschungen stellten bzw. stellen Bundesbehörden bis zur Übernahme der aktuellen EU-Ratspräsidentschaft an (oder haben diese beauftragt), um Zugang zu Ende-zu-Ende-verschlüsselten Daten zu erhalten, die über Messenger-Dienste verschickt werden, und welche beteiligten Elemente (Endgerät, Server und Verschlüsselungsart) stehen dabei im Mittelpunkt?

   a) In welchen Fällen, in denen die Telekommunikation netzseitig durch Netzbetreiber im Inland verschlüsselt ist, haben die betreffenden Firmen in der Vergangenheit mit Behörden des Bundes hinsichtlich des Zugangs zu verschlüsselten Inhalten kooperiert (bitte auch mitteilen, um welche Firmen es sich handelt)?

   b) In welchen Fällen haben Netzbetreiber bei der Erzeugung oder dem Austausch von Schlüsseln mitwirkt und dadurch den Zugriff auf Inhalte ermöglicht (bitte auch mitteilen, um welche Firmen es sich handelt)?

Die Fragen 1 bis 1b werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung unterstützt die Entwicklung, Umsetzung und Nutzung starker Verschlüsselungsverfahren als erforderliches Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Bürgerinnen und Bürgern, Industrie und Gesellschaft.

Die Bundesregierung hat ihre grundsätzliche Haltung zum Thema Verschlüsselung in den Eckpunkten der deutschen Kryptopolitik (Kabinettbeschluss vom 2. Juni 1999) festgelegt.

Danach hält die Bundesregierung an den als „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ bekannten Säulen der deutschen Kryptopolitik fest.

Zugleich vertritt die Bundesregierung die Auffassung, dass trotz der Verbreitung starker Verschlüsselungsverfahren die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden nicht ausgehöhlt werden dürfen. Vor diesem Hintergrund hat der Gesetzgeber in engem Umfang gesetzliche Befugnisse etwa für Maßnahmen der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung geschaffen.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

2. Welche konkreteren Ausführungen kann die Bundesregierung zu ihrer Auffassung machen, wonach Strafverfolgungsbehörden zwar mittels Trojaner-Programmen auch Zugriff zu Inhalten verschlüsselter Telekommunikation erhalten, diese Instrumente jedoch „auch aufgrund eines sehr hohen operativen Aufwands und technischer Schwierigkeiten in der Regel auf wenige Fälle beschränkt“ bleiben (Antwort auf die Schriftliche Fragen 20 und 21 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/25159; bitte mitteilen, worin dieser Aufwand und diese Schwierigkeiten technisch und rechtlich begründet sind)?

Die Bundesregierung geht bei der Beantwortung dieser Frage davon aus, dass diese auf den Einsatz von Programmen zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung durch die gemäß den geltenden gesetzlichen Bestimmungen hierzu befugten Sicherheitsbehörden abzielt. Der Begriff „Trojaner“ ist für solche Instrumente der informationstechnischen Überwachung ungeeignet, wie die Bundesregierung bereits im Rahmen der Beantwortung mehrerer Kleiner Anfragen, beispielsweise auf Bundestagsdrucksache 18/11261 zu Frage 13, Bundestagsdrucksache 19/1434 zu Frage 18 oder Bundestagsdrucksache 19/12465 zu den Fragen 11 bis 11e dargestellt hat.

Bei der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung sind die hierzu befugten Sicherheitsbehörden gemäß geltendem Recht an die jeweiligen inhaltlichen Tatbestandsvoraussetzungen sowie an enge Rahmenbedingungen gebunden. Beispielsweise ist durch technische und organisatorische Maßnahmen sicherzustellen, dass ausschließlich in das informationstechnische System der von dem jeweiligen Beschluss bzw. der jeweiligen Anordnung der Maßnahme betroffenen Person eingegriffen wird.

Hierzu sind im Vorfeld und während der Überwachungsmaßnahme in der Regel aufwändige Untersuchungen zur eindeutigen Identifizierung des zu überwachenden informationstechnischen Systems (Endgeräts) durch die durchführende Sicherheitsbehörde erforderlich. Weiterhin sind vor, während und nach der Durchführung der jeweiligen Maßnahme die Vertraulichkeit, Authentizität und Integrität der Maßnahme sowie der erhobenen und übertragenen Daten zu gewährleisten und es ist sicherzustellen, dass eine Erhebung von Daten auf dem zu überwachenden informationstechnischen System ausschließlich innerhalb des in dem jeweiligen Beschluss bzw. der jeweiligen Anordnung der Maßnahme vorgegebenen Zeitraums erfolgt und sich eventuelle Veränderungen an dem betroffenen System auf das für die Durchführung der Maßnahme erforderliche Mindestmaß beschränken und eventuelle im Rahmen der Durchführung der Maßnahme vorgenommene Veränderungen nach Beendigung der Maßnahme soweit wie möglich rückgängig gemacht werden. Die Umsetzung dieser sowie weiterer Vorgaben zur Gewährleistung von IT-Sicherheit und Datenschutz bei jeder einzelnen der o. g. Überwachungsmaßnahmen führt bei den durchführenden Stellen grundsätzlich zu einem hohen operativen Aufwand und, abhängig von den technischen Rahmenbedingungen, zu technischen Herausforderungen, sodass ein Einsatz der genannten Instrumente in der Regel nur in einem entsprechend beschränkten Umfang möglich ist.

3. Welche „Expertengruppen“, „Expertenprozesse“ oder sonstigen Zusammenschlüsse, die sich mit „Herausforderungen von Verschlüsselung“ und entsprechenden Maßnahmen dagegen befassen sind der Bundesregierung auf EU-Ebene bekannt, und wer nimmt daran teil?

   a) Welche dieser Zusammenschlüsse befassen sich mit „Herausforderungen“ der Ende-zu-Ende-Verschlüsselung von Telekommunikation?

   b) Welche dieser Zusammenschlüsse und Maßnahmen wurden von deutschen Behörden initiiert oder sogar gegründet?

   c) An welchen dieser Zusammenschlüsse und Maßnahmen sind welche deutschen Behörden in welcher Funktion (etwa Leiter, Co-Leiter, Sachverständige) beteiligt?

Die Fragen 3 bis 3c werden gemeinsam beantwortet.

Auf die Antwort zu den Fragen 4, 5 und 9 wird verwiesen.

4. Welche Treffen der „European Expert Group on Cybercrime“ haben nach Kenntnis der Bundesregierung Herausforderungen von Verschlüsselungs- und Anonymisierungsverfahren für Strafverfolgungsbehörden behandelt (Antwort zu Frage 28 auf Bundestagsdrucksache 18/4193), und welche deutschen Behörden haben hierzu welche Präsentationen gehalten?

Die Etablierung einer „European Expert Group on Cybercrime“ war im Rahmen des Operativen Aktionsplans (OAP) 2015 der EMPACT Priorität „Cyberattacks against information systems“ zwar geplant, wurde allerdings nicht realisiert.

5. Welche Treffen der „Freunde der Präsidentschaft zu Cyber“ (FoP Cyber) haben nach Kenntnis der Bundesregierung „Herausforderungen“ von Verschlüsselung für Strafverfolgungsbehörden behandelt, und welche Empfehlungen oder „praktischen Beiträge“ wurden anschließend an die Kommission gerichtet (Ratsdokument 14079/15)?

Die „Freunde der Präsidentschaft zu Cyber“ (FOP Cyber) ist in das Vorbereitungsgremium des Rats der Europäischen Union „Horizontal Working Party on Cyber Issues (HWP Cyber)“ übergegangen.

Das Thema Kryptographie wurde seit 2017 dreimal aufgerufen. Einmal als Gastvortrag durch Vertreterinnen und Vertreter der OECD sowie zweimal als Informationspunkt der EU-Kommission. Es wurden im Anschluss keine „praktischen Beiträge“ an die Kommission gerichtet.

6. Welche Aufgaben übernimmt nach Kenntnis der Bundesregierung die beim Justiziellen Netzwerk für Cyberkriminalität (EJCN) eingerichtete „Beobachtungsstelle für Verschlüsselung“ hinsichtlich einer „Bewältigung der Herausforderungen von Verschlüsselung“ (Ratsdokument 8482/17), und inwiefern gehört dazu auch die Unterstützung bei der Suche nach legislativen Regelungen?

Eine „Beobachtungsstelle für Verschlüsselung“ ist der Bundesregierung unter dieser Bezeichnung nicht bekannt. Auch aus dem in Bezug genommenen Ratsdokument 8482/17 ergibt sich eine solche „Beobachtungsstelle“ nicht.

Allerdings nimmt Europol in Zusammenarbeit mit Eurojust eine Beobachtungsfunktion wahr, um vorausschauend Maßnahmen in Bezug auf Verschlüsselung

zu analysieren. Dazu war und ist das EJCN unterstützend tätig. Der Zweck der Beobachtungsfunktion besteht darin, die jeweils aktuelle Entwicklung im Spannungsfeld zwischen dem legitimen Interesse der Verschlüsselung von privaten Informationen einerseits und der effektiven Strafverfolgung andererseits im Blick zu behalten. Wie sich aus den bislang vorgelegten Berichten ergibt, geht es dabei nicht um konkrete Vorschläge für legislative Regelungen, sondern um eine darstellende Bestandsaufnahme unter Einbeziehung technischer und rechtlicher Fragestellungen (Bericht vom 11. Januar 2019: www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption, Bericht vom 18. Februar 2020: www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption).

7. Was ist der Bundesregierung über Beteiligte eines „Reflektionsprozesses“ zur Rolle der Verschlüsselung in strafrechtlichen Ermittlungen bei der Kommission bekannt (Ratsdokument 6890/17), für welche Zwecke hat die Kommission einen „Expertenprozess“ gestartet (https://www.consilium.europa.eu/de/meetings/jha/2017/06/08-09), und inwiefern sind diese Prozesse inzwischen zusammengeführt worden?

Wie in der „Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat, Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Elfter Fortschrittsbericht“ (COM (2017) 608 final) vom 18. Oktober 2017 beschrieben, hat die Kommission infolge eines Aufrufs des JI-Rats im Dezember 2016 die Rolle der Verschlüsselung in strafrechtlichen Ermittlungen im Rahmen eines „Reflektions-“ bzw. „Expertenprozesses“ erörtert. Dabei wurden technische und rechtliche Fragen thematisiert.

Einzelheiten zu den Beteiligten, dem Ablauf, den Zwecken und den Ergebnissen können dem 11. Fortschrittsbericht entnommen werden, der abrufbar ist unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52017DC0608 (zuletzt 13. Januar 2021).

8. Wann hat die Kommission nach Kenntnis der Bundesregierung ihren Bericht zu den technischen und juristischen Arbeitsgruppen vorgelegt, und in welchem Ratsdokument wurde dieser verteilt (WK 528/2017 INIT)?

   a) Welche wesentlichen Ergebnisse, Schlussfolgerungen und Empfehlungen hat die Kommission hierzu mitgeteilt?

   b) Welche weiteren Maßnahmen wurden anschließend von der Kommission vorgeschlagen?

Die Fragen 8 bis 8b werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Kommission hat in der „Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat, Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Elfter Fortschrittsbericht“ (COM (2017) 608 final) vom 18. Oktober 2017 zu den Arbeitsgruppen berichtet. Ein weiterer Bericht ist der Bundesregierung nicht bekannt. Im Übrigen wird auf die Antwort zu Frage 7 verwiesen.

9. Welche „Expertenworkshops“ haben nach Kenntnis der Bundesregierung bei Europol zu Verschlüsselung stattgefunden (Antwort auf die Schriftliche Frage 13 der Abgeordneten Inge Höger auf Bundestagsdrucksache 18/12703 sowie Antwort auf die Schriftliche Frage 19 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/695), welches deutsche Personal aus welchen Abteilungen war dort vertreten, und welche Präsentationen haben diese gehalten?

Es wird zunächst auf die Antworten der Bundesregierung auf die Schriftliche Frage 13 auf Bundestagsdrucksache 18/12703 sowie auf die Schriftliche Frage 19 auf Bundestagsdrucksache 19/695 verwiesen. Der genannte Workshop am 24. Mai 2017 fand unter Beteiligung des Bundeskriminalamtes (BKA), der Workshop am 5. Februar 2018 unter Beteiligung des BKA und des Bundesministeriums des Innern, für Bau und Heimat statt, ohne dass von dort eine Leitungsfunktion oder einzelne Präsentationen übernommen wurden.

Der Bundesregierung ist darüber hinaus bekannt, dass das Joint Research Centre (JRC) der EU-Kommission gemeinsam mit Europol an der Entwicklung der neuen Europol-Dekryptierungsplattform mitgewirkt hat.

Darüber hinaus findet am JRC regelmäßig der Law Enforcement Authorities (LEA) Decryption Workshop statt, in dem technische Expertinnen und Experten, unter anderem aus den Behörden der Mitgliedstaaten, die Möglichkeit zum Austausch über aktuelle Entwicklungen und Projekte haben.

Ferner hat sich die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) an der Online-Plattform Europol Platform for Experts (EPE) beteiligt, auf der unter anderem Themen im Kontext von „Herausforderungen von Verschlüsselungen“, dazu gehören auch die Herausforderungen der Ende-zu-Ende-Verschlüsselung, besprochen werden. Die ZITiS hat keinerlei Leitungsfunktion in diesem Zusammenhang übernommen, sondern hat sich mit einzelnen Experten an der EPE beteiligt.

Darüber hinaus wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

10. Welche deutschen Behörden oder Bundesministerien nehmen an der „Ständigen Gruppe der Leiter der Abhörabteilungen“ teil (Ratsdokument 11517/20), und auf welchen Treffen hat sich diese mit verschlüsselter Kommunikation befasst?

Es wird auf die Antwort der Bundesregierung zu den Fragen 2, 6 und 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/24592 verwiesen.

* Das Bundesministerium des Innern, für Bau und Heimat 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.

11. Was ist der Bundesregierung über den Fortgang von Plänen bekannt, wonach Europol eine Spionagesoftware zum Eindringen in Endgeräte der digitalen Kommunikation (Trojaner) entwickeln und den Behörden der Mitgliedstaaten als Dienstleistung zur Verfügung stellen soll (Ratsdokument WK 12742/2018)?

    a) Wer nimmt hierzu an entsprechenden Diskussionen oder Treffen teil?

    b) Welche Pilotprojekte wurden hierzu geplant oder beschlossen, bzw. aus welchen Gründen wurden diese wieder verworfen?

    c) Inwiefern ist die nichtöffentliche Ausschreibung für die technische „Lösung“ bereits erfolgt, und wer erhielt den Zuschlag?

12. Was ist der Bundesregierung darüber bekannt, inwiefern die Kommission eine Machbarkeitsstudie und/oder ein Pilotprojekt zum Einsatz eines Europol-Trojaners mit freiwilligen Mitgliedstaaten startet und/oder finanziert?

Die Fragen 11 bis 12 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Zum Ausbau von Entschlüsselungskapazitäten bei Europol wird zunächst auf die Antwort der Bundesregierung auf die Schriftliche Frage 14 auf Bundestagsdrucksache 19/4734 verwiesen. Die dort beschriebene Aufstockung von Mitteln zur Stärkung der „Entschlüsselungsfähigkeiten“ bei Europol betrifft nach Kenntnis der Bundesregierung die forensische Entschlüsselung von sichergestellten elektronischen Beweismitteln. Im Jahr 2018 waren für die Einrichtung der Entschlüsselungsplattform 5 Mio. Euro aus dem Europol-Haushalt vorgesehen. Von einer durch Europol zu entwickelnden sog. „Spionagesoftware“ zum Eindringen in Endgeräte der digitalen Kommunikation, die den Behörden der Mitgliedstaaten als Dienstleistung zur Verfügung gestellt würde, ist der Bundesregierung nichts bekannt.

13. Wie oft hat das BKA die Fähigkeiten von Europol zum Entschlüsseln von passwortgeschützten Speichermedien seit Bestehen der „Entschlüsselungsplattform“ genutzt, und in welchen Fällen hat das BKA diese Ersuchen für andere deutsche Polizeibehörden als Kontaktstelle vermittelt?

Der Bundesregierung ist diese bei Europol eingerichtete Entschlüsselungsplattform bekannt. Diese wird in Einzelfällen vom BKA in Ermittlungsverfahren genutzt.

14. Was ist der Bundesregierung darüber bekannt, auf welche Weise und in welchen Projekten das „EU-Innovationszentrum für innere Sicherheit“ bei Europol im Bereich der Sicherheitsforschung mit Verschlüsselung befasst ist?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

15. Was ist der Bundesregierung darüber bekannt, auf welchen EU-US-Ministertreffen der „Umgang mit Verschlüsselung“ behandelt wurde (Ratsdokument 15062/16), und welche Absprachen wurden dort hinsichtlich eines abgestimmten Vorgehens getroffen?

Nach Kenntnis der Bundesregierung findet zum Thema „Umgang mit Verschlüsselung“ bei den halbjährlichen EU-US Ministerreffen regelmäßig ein Meinungsaustausch statt. Von Seite der Mitgliedstaaten nimmt an diesen Tref-

fen jedoch lediglich die amtierende und die kommende EU-Ratspräsidentschaft teil. Während der deutschen Ratspräsidentschaft fiel das Treffen Corona-bedingt aus. Beim Treffen während der kroatischen Ratspräsidentschaft, das im Videoformat stattfand, wurden keine Absprachen im Sinne der Fragestellung getroffen.

16. Welche „Expertengruppen“, „Expertenprozesse“ oder sonstigen Zusammenschlüsse, die sich mit „Herausforderungen von Verschlüsselung“ und entsprechenden Maßnahmen dagegen befassen, waren an der Ausarbeitung oder Abstimmung der vom deutschen Ratsvorsitz initiierten „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ (Ratsdokument 13245/20) direkt oder indirekt beteiligt?

Die deutsche Ratspräsidentschaft wurde von den Mitgliedstaaten im COSI am 23. September 2020 mandatiert, eine Initiative zum Thema Verschlüsselung ins Leben zu rufen. Der Rat hat hiernach am 14. Dezember 2020 eine Entschließung zur Verschlüsselung mit dem Titel „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ verabschiedet.

17. Was ist der Bundesregierung darüber bekannt, inwiefern Internetdienstleister schon jetzt an einem Dialog über technische Maßnahmen für den Zugang zu Ende-zu-Ende-verschlüsselter Kommunikation beteiligt sind (etwa im EU-Internetforum), und von wem geht diese Initiative aus?

Die Internetdienstanbieter stehen bereits wiederkehrend anlassbezogen und anlassunabhängig in einem intensiven Austausch mit den Sicherheitsbehörden. Ziele dieser Meetings sind die Diskussion aktueller Problemstellungen, die gemeinsame Erarbeitung von Lösungen und damit die kontinuierliche Verbesserung der Zusammenarbeit. Die Gesprächsformate mit ausländischen Diensteanbietern beziehen sich jedoch allein auf Auskunftsersuchen zu Bestandsdaten.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, 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