Deutscher Bundestag **Drucksache 19/25264**

19. Wahlperiode 15.12.2020

Kleine Anfrage

der Abgeordneten Andrej Hunko, Michel Brandt, Sevim Dağdelen, Ulla Jelpke, Cornelia Möhring, Niema Movassat, Zaklin Nastic, Dr. Alexander S. Neu, Thomas Nord, Tobias Pflüger, Martina Renner und der Fraktion DIE LINKE.

EU-Maßnahmen gegen Verschlüsselung unter deutscher Beteiligung

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 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.

Wir fragen die Bundesregierung:

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)?

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 Bundestagsdruck-

sache 19/25159; bitte mitteilen, worin dieser Aufwand und diese Schwierigkeiten technisch und rechtlich begründet sind)?

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?

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?

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)?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

Berlin, den 8. Dezember 2020

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

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