Deutscher Bundestag **Drucksache 18/7024**

18. Wahlperiode 10.12.2015

Kleine Anfrage

der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Frank Tempel, Jan van Aken, Annette Groth, Dr. André Hahn, Inge Höger, Ulla Jelpke, Jan Korte, Dr. Petra Sitte und der Fraktion DIE LINKE.

Europäische Anstrengungen zur möglichen Aushebelung verschlüsselter Telekommunikation

Im November 2015 hat der luxemburgische Ratsvorsitz ein Papier mit einem Sachstand an die Mitgliedstaaten verschickt, in dem Herausforderungen durch die „Kommunikationskanäle des Internets und die zahlreichen sozialen Medien“ skizziert werden (Ratsdok. 14677/15). Neue „verschlüsselungsbasierte Technologien“ würden die „Durchführung effektiver Ermittlungen“ zunehmend erschweren oder verhindern. Von besonderer Bedeutung seien diese auch bei „Antiradikalisierungsmaßnahmen“. Das Papier fordert unter anderem eine „effektive Vorratsdatenspeicherung“. In einem weiteren Dokument fragt der luxemburgische Ratsvorsitz den Bedarf für entsprechende Schritte der Kommission ab (Ratsdok. 14369/15). Als weitere Hindernisse für Strafverfolger werden die „private Nutzung des Live-Streamings“, das Darknet und Anonymisierungswerkzeuge genannt. „Entscheidende elektronische Beweismittel“ gingen verloren, wenn den zuständigen Behörden keine geeigneten Mittel zur Verfügung gestellt würden.

Im Januar 2015 forderte der EU-Anti-Terror-Koordinator Gilles de Kerchove, Internet- und Telekommunikationsanbieter zum Einbau von Hintertüren für verschlüsselte Kommunikation zu zwingen (www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf). Im März 2015 warnte der Direktor des Europäischen Polizeiamtes (Europol), Rob Wainwright, vor der zunehmenden Nutzung von Verschlüsselungstechnologien. Verschlüsselung sei demnach „eines der Hauptinstrumente von Terroristen und Kriminellen“. Im September 2015 trug der stellvertretende Leiter der Operationsabteilung von Europol, Wil van Gemert, auf einer Konferenz der europäischen Polizeichefs den Bericht einer Arbeitsgruppe zu „terroristischen Online-Bedrohungen“ vor (www.statewatch.org/news/2015/nov/eu-council-eppc-2015-report-09-2015.pdf). Demnach müssten vor allem die „Hindernisse von Anonymisierung und Verschlüsselung“ überwunden werden. An der Arbeitsgruppe nahmen unter anderem Behörden aus Österreich, Dänemark, Ungarn, Deutschland und Spanien teil. Sie raten zu mehr Kooperation mit dem „privaten Sektor“, darunter Providern und Diensteanbietern, um an verschlüsselte Inhalte und den Zugang zu Servern zu gelangen.

Zum zweiten Mal hat Europol im Herbst einen Lagebericht zu Cyberkriminalität herausgegeben, in dem das Thema Verschlüsselung und Anonymisierung ausführlich behandelt wird (www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015). Zu den Erschwernissen für die Behörden zählt Europol auch „Anti-Forensik-Werkzeuge“, darunter Software zum Überschreiben von Inhalten oder Betriebssysteme, die von Wechselmedien gestartet

werden. Diese seien bei Kriminellen nicht mehr die Ausnahme, sondern die Regel. In Ermittlungen würden jedoch in „zunehmendem Ausmaß“ digitalisierte Daten benötigt. Laut Europol seien die Ermittlerinnen und Ermittler in drei Vierteln aller Fälle mit verschlüsselten Inhalten konfrontiert. Namentlich genannt werden die Anwendungen TrueCrypt und BitLocker sowie PGP, dessen zunehmende Nutzung von den Behörden der Mitgliedstaaten bestätigt worden sei. Internetanbieter und Plattformen wie WhatsApp, iMessage, Facebook, Facetime, Google und Yahoo würden zudem die voreingestellte Ende-zu-Ende-Verschlüsselung implementieren. Zwar sei dies für den „öffentlichen und privaten Sektor“ zu begrüßen, jedoch stelle sich die Frage nach der Bedeutung dieser Entwicklung für Regierungen und Strafverfolgungsbehörden.

Der Bericht schlägt mehrere Maßnahmen vor. „Gesetzgeber“ und Abgeordnete müssten „mit der Industrie und der Forschung“ brauchbare Lösungen entwickeln, die einerseits die Privatheit und Urheberrechte respektieren, den Behörden jedoch ausreichend Handhabe zur Bekämpfung von „kriminellen oder nationalen Sicherheitsbedrohungen“ bereitstellten. Auch Ermittlungen wegen Kinderpornografie seien hiervon betroffen. Zu den Empfehlungen gehört die Entwicklung von Techniken, um bei einer polizeilichen Razzia Daten aus verschlüsselten, aber noch nicht ausgeschalteten Systemen rekonstruieren zu können. Die Behörden sollten außerdem eine „zentrale Datenbank“ mit „VPN- und Proxy-Diensten“ anlegen, die bevorzugt von „Cyberkriminellen“ genutzt würden.

Nun will sich auch die Gruppe „Freunde der Präsidentschaft zu Cyber“ (FoP Cyber) mit dem Umgehen von Verschlüsselung befassen (www.statewatch.org/news/2015/dec/eu-council-cosi-int-sec-14079-15.pdf). Auch dort ist die Rede von Ermittlungshindernissen, die es zu überwinden gelte. Die Gruppe kündigt an, die zukünftige Entwicklung im Auge zu behalten. Jeder teilnehmende Mitgliedstaat entsendet einen „Cyber-Attaché“ nach Brüssel. In den zwei letzten Treffen dieser hohen Beamtinnen und Beamten im Oktober und November 2015 ging es unter anderem um den „Missbrauch von Verschlüsselung und Anonymität“ und entsprechende Gesetzeslücken. Die Gruppe will nun für öffentliches Bewusstsein zum Thema sorgen, Handlungsempfehlungen geben und die Kommission mit „praktischen Beiträgen“ zu neuen Gesetzgebungsvorschlägen versorgen.

Im Bundesministerium des Inneren werden die europäischen Anstrengungen ausdrücklich begrüßt (Bundestagsdrucksache 18/5144). Das „Streben nach einer abgeschirmten, klandestinen Übermittlung von Informationen“ sei in vielen Phänomen- und Kriminalitätsbereichen ein „prägendes Wesensmerkmal im Kommunikationsverhalten“. Dieses hätte zum Ziel, „die staatlichen Aufklärungs- und Bekämpfungsmaßnahmen ins Leere laufen zu lassen“. Für den Zugriff auf nutzerseitig verschlüsselte Kommunikation bestehe jedoch derzeit keine Rechtsgrundlage. Zur Suche nach den „unterschiedlichen Bedürfnissen im Verhältnis Datenschutz zu Gefahrenabwehr und Strafverfolgung“ sei deshalb „jedweder Dialog mit Internet-Diensteanbietern“ zu begrüßen. Als nächsten Schritt hat die EU am 3. Dezember 2015 den offiziellen Start des „Forums der Internetdienstleister“ verkündet. In der neuen Gemeinschaft organisieren sich die EU-Innenministerinnen und EU-Innenminister mit Internetkonzernen. Nach über einem Jahr Vorbereitung wird eine Zusammenarbeitsform installiert, die eine möglichst schnelle Beseitigung unliebsamer Internetinhalte ermöglichen soll. Zu den weiteren „Möglichkeiten der praktischen Zusammenarbeit“ zählt der Umgang mit Verschlüsselungstechniken.

Wir fragen die Bundesregierung:

1. Inwiefern sieht auch die Bundesregierung neue Herausforderungen durch die „Kommunikationskanäle des Internets und die zahlreichen sozialen Medien“ hinsichtlich „verschlüsselungsbasierter Technologien“ und deren Verhinderung der „Durchführung effektiver Ermittlungen“?

2. Wie hat sich die Bundesregierung zu einem entsprechenden Papier des luxemburgischen Ratsvorsitzes positioniert?
3. Welche „Antiradikalisierungsmaßnahmen“ sind nach Kenntnis der Bundesregierung in dem Papier gemeint?
4. Wie hat sich die Bundesregierung gegenüber dem Ratsvorsitz zur Frage des Auftrages der Kommission hinsichtlich der Vorratsdatenspeicherung positioniert, und wie wurden die Fragen des versandten Fragebogens beantwortet?
5. Welche Behörden (auch deutsche) haben nach Kenntnis der Bundesregierung an einer Arbeitsgruppe zu „terroristischen Online-Bedrohungen“ teilgenommen?
   a) Auf welche Weise hat sich diese Arbeitsgruppe auch mit Anonymisierung und Verschlüsselung befasst?
   b) Welche weiteren Teilnehmenden (auch zur Beratung) waren eingebunden?
   c) Wie lange soll die Arbeitsgruppe bestehen?
6. Welche konkreten Vorschläge zur Überwindung entsprechender „Hindernisse“ werden in dem Bericht der Arbeitsgruppe gemacht?
   a) Sofern zu mehr Kooperation mit Providern und Diensteanbietern geraten wird, um an verschlüsselte Inhalte und den Zugang zu Servern zu gelangen, wie könnte dies aus Sicht der Bundesregierung umgesetzt werden?
   b) Welche Schlussfolgerungen zieht die Bundesregierung aus dem Bericht, und welchen der dort vorgeschlagenen Maßnahmen stimmt sie zu?
   c) Was ist nach Kenntnis der Bundesregierung damit gemeint, wenn Europol fordert, eine „zentrale Datenbank“ mit „VPN- und Proxy-Diensten“ anzulegen, und wo könnte diese angesiedelt werden?
7. Inwiefern stehen auch Bundesbehörden vor dem Problem der zunehmenden Verwendung von „Anti-Forensik-Werkzeugen“, darunter Software zum Überschreiben von Inhalten oder Betriebssysteme, die von Wechselmedien gestartet werden?
8. In welcher Größenordnung sind deutsche Behörden nach Kenntnis der Bundesregierung mit verschlüsselten Inhalten konfrontiert?
9. Welche der Werkzeuge werden dabei besonders häufig eingesetzt?
10. Auf welche Weise hat sich nach Kenntnis der Bundesregierung die Gruppe „FoP Cyber“ mit dem Thema Verschlüsselung befasst?
11. Auf welche Weise und mit welchen Initiativen und Maßnahmen will die FoP Cyber das Thema weiter behandeln?
12. Welche Mitgliedstaaten oder sonstigen Teilnehmenden haben einen „Cyber-Attaché“ zur FoP Cyber entsandt?
13. In welchen Treffen der FoP Cyber hat diese nach Kenntnis der Bundesregierung das Thema Verschlüsselung behandelt, und wer trug dazu vor (bitte auch das Thema der Präsentationen benennen)?
   a) Welche „Gesetzeslücken“ wurden identifiziert?
   b) In welchen weiteren Treffen steht das Thema auf der Tagesordnung?
14. Aus welchen Erwägungen nehmen nach Kenntnis der Bundesregierung auch der für die Sicherheits- und Verteidigungspolitik zuständige Europäische Auswärtige Dienst (EAD) sowie die Europäische Verteidigungsagentur (EDA) an der FoP Cyber teil?

15. Auf welche Weise sollten bzw. könnten der EAD und die EDA aus Sicht der Bundesregierung das Thema Verschlüsselung behandeln?

16. Auf welche Weise will die FoP Cyber nach Kenntnis der Bundesregierung für öffentliches Bewusstsein zum Thema sorgen, Handlungsempfehlungen geben und die Kommission mit „praktischen Beiträgen“ zu neuen Gesetzgebungsvorschlägen versorgen?

17. Welche Haltung vertritt die Bundesregierung hinsichtlich der Notwendigkeit neuer Regelungen zur Sicherstellung von digitalen Beweismitteln „e-evidence“?

    a) Inwiefern sollte hierzu auch die Übermittlung von Daten durch Internetanbieter zu Polizeien und Geheimdiensten erleichtert werden?

    b) Inwiefern sieht die Bundesregierung entsprechende Defizite auch in der grenzüberschreitenden Zusammenarbeit mit den USA, und auf welche Weise wird das Thema in den nächsten Monaten behandelt?

    c) Was ist der Bundesregierung darüber bekannt, inwiefern die US-Regierung mit EU-Mitgliedstaaten darüber verhandeln möchte oder bereits verhandelt, dass US-Strafverfolger zukünftig bei EU-Internetanbietern Auskunftsverlangen zu Telekomunikationsdaten stellen und womöglich auch die Echtzeit-Telekommunikationsüberwachung verlangen dürfen?

18. Wie viele Ersuchen zur Entfernung von Internetinhalten hat die „Meldestelle für Internetinhalte“ bei Europol nach Kenntnis der Bundesregierung bereits erhalten, und wie vielen der Ersuchen wurde nachgekommen?

19. Inwiefern wird auch die Bundesregierung dem Aufruf der “Meldestelle” nachkommen, mehr „nationale Experten“ zu entsenden?

20. Welche privaten Teilnehmenden des am 3. Dezember 2015 in Brüssel gestarteten „Forums der Internetdienstleister“ sind der Bundesregierung durch ihre eigene Teilnahme bekannt (Plenarprotokoll 18/142), und aus welchem Grund wurden entgegen früheren Ankündigungen der Kommission keine Vertreter der Zivilgesellschaft eingeladen (Antwort der Kommission auf die Anfrage von Cornelia Ernst, MEP, Kommissionsdokument E-006551/2015)?

21. Inwiefern hält auch die Bundesregierung die Teilnahme von Vertretern der Zivilgesellschaft für entbehrlich?

22. Welche Veränderungen werden sich aus Sicht der Bundesregierung durch die Umwandlung des „Radicalisation Awareness Network” in ein „Centre of Excellence“ für die Arbeit des Zentrums ergeben?

23. Bei welchen vorbereitenden Treffen des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister“ wurde das Thema Verschlüsselung nach Kenntnis der Bundesregierung behandelt, und wer trug dazu vor (bitte auch das Thema der Präsentationen benennen)?

    a) Welche „Möglichkeiten der praktischen Zusammenarbeit“ wurden dabei bislang behandelt, und inwieweit hält die Bundesregierung diese für praktikabel?

    b) Was ist der Bundesregierung darüber bekannt, auf welchen zukünftigen Treffen das Thema Verschlüsselung behandelt werden soll?

24. Was ist der Bundesregierung über Pläne bekannt, die am Forum teilnehmenden Internetanbieter dafür zu gewinnen, bei besonderen terroristischen Vorkommnissen die Schaltung von Werbung gratis anzubieten, um möglichst viele „Gegendiskurse“ produzieren zu können, und welche Haltung vertritt sie hierzu?

25. Was ist der Bundesregierung darüber bekannt, welche großen US-Internetdienstleister personenbezogene Nutzerdaten, IP-Adressen oder Informationen über besuchte Webseiten auch ohne Rechtshilfeersuchen herausgeben?
26. Welche Haltung vertritt die Bundesregierung zu der Frage, ob der Zugang großer US-Internetdienstleister in europäischen Märkten an die Frage der Herausgabe personenbezogener Nutzerdaten gekoppelt sein sollte?
27. Was ist der Bundesregierung über Forderungen einzelner EU-Mitgliedstaaten nach einem generellen Verbot von Verschlüsselung bekannt, und welche Auswirkungen hätte dies auf die deutsche Haltung zu Verschlüsselung?
28. Was ist der Bundesregierung über Forderungen einzelner EU-Mitgliedstaaten bekannt, wonach alle Anbieter von Verschlüsselungstechnologien zur Einrichtung von Hintertüren für Strafverfolger gezwungen werden sollten, und welche Auswirkungen hätte dies auf die deutsche Haltung zu Verschlüsselung?
29. In welchen der oben genannten Zusammenarbeitsformen wurde nach Kenntnis der Bundesregierung auch thematisiert, den gewünschten Zugang von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation durch den verstärkten (grenzüberschreitenden) Einsatz staatlich genutzter Trojanerprogramme zu ermöglichen?
    a) Wer trug hierzu entsprechende Ausführungen vor?
    b) Inwiefern wurde bei den Vorträgen und Diskussionen auch über EU-weit oder international zu vereinheitlichende Regelungen verwiesen, und um welche handelt es sich dabei?
30. Auf welche Weise wäre eine EU-weit oder international zu vereinheitlichende Regelung des (grenzüberschreitenden) Einsatzes staatlich genutzter Trojanerprogramme aus Sicht der Bundesregierung eine geeignete Möglichkeit zur Umsetzung des gewünschten Zugangs von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation?
31. Was ist der Bundesregierung darüber bekannt, inwiefern auch die EU-Agentur Eurojust in Anstrengungen eingebunden ist, den Kontakt zu Internetdienstleistern hinsichtlich der Entfernung von Inhalten oder der Strafverfolgung zu verbessern, und welche Internetkonzerne wurden zu einem entsprechenden Treffen im Oktober 2015 eingeladen (www.statewatch.org/news/2015/nov/eu-council-c-t-implementation-strategy-14438-15.pdf)?
32. Wann soll die europäische Ermittlungsanordnung nach Kenntnis der Bundesregierung in nationales Recht umgesetzt werden, und inwiefern hält die Bundesregierung die in der Richtlinie geregelte grenzüberschreitende Anordnung von Zwangsmaßnahmen schon jetzt für überarbeitungswürdig?
33. Welche Priorisierungen hat die Bundesregierung in Reaktion auf das Ratsdok. 14369/15 vorgenommen (bitte die Punkte kurz anreißen)?

Berlin, den 10. Dezember 2015

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

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