



Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117

FAX +49 (0)30 18 681-11019

INTERNET www.bmi.bund.de

DATUM 6. April 2017

BETREFF **Kleine Anfrage des Abgeordneten Andrej Hunko . a. und der Fraktion
DIE LINKE.**

**Maßnahmen des EU-Internet Forum zur Kontrolle des Internet und
verschlüsselter Telekommunikation**

BT-Drucksache 18/11676

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte
Antwort in 4-facher Ausfertigung.

Mit freundlichen Grüßen
in Vertretung

Dr. Emily Haber

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin

VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof

Bushaltestelle Berlin Hauptbahnhof

Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.

Maßnahmen des EU-Internet Forum zur Kontrolle des Internet und verschlüsselter Telekommunikation

BT-Drucksache 18/11676

Vorbemerkung der Fragesteller:

Als erster Industriepartner hat Facebook damit begonnen, jeden Upload von Bilddaten auf „gewalttätige terroristische Inhalte“ zu analysieren. Sind die Fotos oder Videos in einer gemeinsam mit anderen Internetfirmen geführten Datenbank als „terroristisch“ oder „extremistisch“ markiert, wird der Upload automatisch verhindert. Die Inbetriebnahme des als „Prototyp“ bezeichneten Uploadfilters erfolgte anlässlich eines Besuchs des EU-Innenkommissars Dimitris Avramopoulos am Freitag bei Facebook, Twitter und Youtube (Pressemitteilung der Europäischen Kommission vom 10. März 2017, „EU Internet Forum: progress on removal of terrorist content online“). Die drei Firmen hatten ihre Mitarbeit im sogenannten EU-Internet Forum erklärt. Dort sollen die Internetunternehmen dazu gedrängt werden, das Internet stärker zu kontrollieren. Es ist unklar, wo die Datenbank mit Hashwerten der zu entfernenden Internetinhalte geführt wird. Vermutlich werden dort auch IP-Adressen der für den Upload benutzten Kommunikationsgeräte gespeichert. Die Personendaten könnten von den Internetfirmen oder Polizeibehörden dazu benutzt werden, andere Accounts der gleichen NutzerInnen aufzuspüren.

Neben der Entfernung von Inhalten werden im EU-Internet Forum weitere Maßnahmen im Bereich der Cybersicherheit und der Herausgabe elektronischer Beweismittel beschlossen. Seit der Gründung des Forums im Dezember 2015 steht der Zugang von Ermittlungsbehörden zu verschlüsselter Telekommunikation auf der Agenda. Anfangs hatte sich die Europäische Kommission laut dem deutschen Bundesinnenministerium hierzu zurückgehalten. Beim Treffen letzte Woche wurde das Thema „Verschlüsselung“ laut einer Pressemitteilung der Kommission jedoch behandelt. Mit von der Partie war der EU-Koordinator für die Terrorismusbekämpfung, Gilles de Kerchove, der seit zwei Jahren in mehreren Papieren auf die Mitarbeit der Firmen bei der Entschlüsselung drängt.

Vorbemerkung:

Zur Zielsetzung des EU Internet Forums verweist die Bundesregierung auf die Antwort zur Kleinen Anfrage der Fraktion DIE LINKE. auf BT-Drs. 18/11578 vom 20. März 2017. In diesem Zusammenhang teilt die Bundesregierung nicht die Auffassung der Fragesteller, wonach die Unternehmen im EU Internet Forum „dazu gedrängt werden, das Internet stärker zu kontrollieren“. Ferner ist es nach dem Kenntnisstand der Bundesregierung unzutreffend, dass „seit der Gründung des Forums im Dezember 2015 (...) der Zugang von Ermittlungsbehörden zu verschlüsselter Telekommunikation auf der Agenda“ gestanden habe.

1. An welchen Treffen des EU Internet Forums (auch Unterarbeitsgruppen) haben der Ständige Vertreter der Bundesrepublik Deutschland bei der Europäischen Union bzw. dessen Stab in 2017 teilgenommen?

Zu 1.

Im Jahr 2017 hat der Ständige Vertreter der Bundesrepublik Deutschland bei der Europäischen Union (EU) bzw. dessen Stab bei keinem Treffen des EU Internet Forums teilgenommen.

2. Was ist der Bundesregierung darüber bekannt, auf welche Weise und mit welchem Werkzeug Facebook oder andere Anbieter Sozialer Netzwerke damit begannen, jeden Upload von Bilddaten auf „gewalttätige terroristische Inhalte“ zu analysieren?

3. Wann wollen welche weiteren Internetanbieter ebenfalls mit der Einführung des Uploadfilters beginnen?

Zu 2. und 3.

Dazu liegen der Bundesregierung keine Kenntnisse vor.

4. Wo wird nach Kenntnis der Bundesregierung die Datenbank des Uploadfilters mit Hashwerten der zu entfernenden Internetinhalte geführt?

Zu 4.

Nach Kenntnis der Bundesregierung wird die Datenbank bei den Unternehmen geführt.

5. Inwiefern werden in der Datenbank auch IP-Adressen der für den Upload benutzten Kommunikationsgeräte gespeichert?

Zu 5.

Dazu liegen der Bundesregierung keine Kenntnisse vor.

6. Welche Firmen oder Behörden haben Zugriff auf diese personenbezogenen Daten?

Zu 6.

Nach Kenntnis der Bundesregierung hätten die Unternehmen Zugriff auf die IP-Adressen der für den Upload benutzten Kommunikationsgeräte, sofern diese (siehe Antwort zu Frage 5) gespeichert werden sollten.

7. Wie viele Online-Inhalte sind nach Kenntnis der Bundesregierung derzeit in der Europol-Auswertedatei „Check the Web“ gespeichert (bitte sowohl gespeicherte Dateien als auch die Gesamtzahl der Einträge angeben)?

Zu 7.

Mit Stand vom 24. März 2017 waren 14.301 Dateien (Videos / Audios, Statements, Publikationen) im Portal „Check the Web“ gespeichert. Mit weiteren 1.675 Einträgen (wie z. B. Websites, terroristische Organisationen) waren zum Erhebungszeitpunkt insgesamt 15.976 Datensätze im Portal erfasst.

8. Was ist der Bundesregierung darüber bekannt, mit welchen Firmen und Angehörigen der US-Regierung sich der EU-Innenkommissar Dimitris Avramopoulos und der EU-Koordinator für die Terrorismusbekämpfung, Gilles de Kerchove, sowie die zuständigen Minister des derzeitigen und künftigen Ratsvorsitzes bei ihrer jüngsten Reise „im Nachgang zu dem EU-Internet Forum“ in den Vereinigten Staaten getroffen haben (Pressemitteilung Europäische Kommission vom 10. März 2017, „EU Internet Forum: progress on removal of terrorist content online“)?

9. Was ist der Bundesregierung über anvisierte Maßnahmen des EU-Innenkommissars und des EU-Koordinators für die Terrorismusbekämpfung sowie der von ihnen besuchten Unternehmen im Bereich der Cybersicherheit und der Herausgabe elektronischer Beweismittel bekannt?

10. Welche sonstigen „Bereiche für die weitere Zusammenarbeit“ wurden nach Kenntnis der Bundesregierung bei den Treffen identifiziert?

Zu 8. bis 10.

Die Fragen 8, 9 und 10 werden zusammen beantwortet. Der Bundesregierung liegen keine Informationen vor, die über die Inhalte der Pressemitteilung hinausgehen.

11. Bezüglich welcher Aspekte wurde nach Kenntnis der Bundesregierung bei den Unterredungen des EU-Innenkommissars und des EU-Koordinators für die Terrorismusbekämpfung mit den von ihnen besuchten Unternehmen auch der Zugang von Ermittlungsbehörden zu verschlüsselter Telekommunikation behandelt?

- a) Welche Maßnahmen wurden hierzu erörtert und/ oder beschlossen?
- b) In welchen Ratsarbeitsgruppen oder sonstigen EU-Gremien wurden die deutsch-französischen Papiere gegen uneingeschränkte Verschlüsselung der Telekommunikation vom Sommer 2016 weiter behandelt oder beraten (netzpolitik.org vom 23. August 2016, „Innenminister fordern Hintertüren gegen Verschlüsselung – in der französischen Version der gemeinsamen Erklärung“)?
- c) Inwiefern trifft es zu, dass das Bundesjustizministerium einen Vorschlag für eine Ergänzung des Paragraphen 100a erarbeitet, um diesen als Rechtsgrundlage für das Eindringen in Nutzeraccounts der Messenger Whatsapp oder Telegram nutzen zu können (Süddeutsche Zeitung vom 13. März 2017, „Geheime Mitleser“)?

Zu 11 und a)

Auf die Antwort zu den Fragen 8, 9 und 10 wird verwiesen.

b)

Auf die Antwort zu Frage 12 wird verwiesen.

c)

Das Bundesministerium der Justiz und für Verbraucherschutz erarbeitet derzeit keine Ergänzung von § 100a der Strafprozessordnung, um diesen als Rechtsgrundlage für das in der Süddeutschen Zeitung beschriebene Verfahren nutzen zu können.

12. Was ist der Bundesregierung über den Fortgang des Reflexionsprozesses der Europäischen Kommission und der EU-Mitgliedstaaten sowie den relevanten Agenturen bekannt, den zuständigen Verfolgungsbehörden den leichteren Zugang zu verschlüsselter Kommunikation zu ermöglichen (<http://gleft.de/1DY>)?

Zu 12

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“ stand auf der Tagesordnung des Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (CATS) am 8. März 2017 sowie des JI-Rates am 27./28. März 2017. Darüber hinaus geht die Bundesregierung davon aus, dass das Sujet auch weiterhin in Sitzungen verschiedener Ratsarbeitsgruppen, z.B. der „Horizontal Working Party on Cyber Issues“ (HWP), so wie zuletzt am 22. März 2017 thematisiert wird.

13. Inwiefern wird nach Kenntnis der Bundesregierung auch das Problem der Carrier-Grade Network Address Translation und die damit verbundene schwierige Zuordnung externer IPv4-Adressen (Drucksache 18/10948, Frage 17) auf Ebene des EU Internet Forums erörtert?

Zu 13.

Auf die Antwort der Bundesregierung zu Frage 12 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11578 vom 20. März 2017 wird verwiesen.

14. Worin besteht nach Kenntnis der Bundesregierung das von der Europäischen Kommission gestartete „EU Civil Society Empowerment Programme“ (CSEP) und wie wird es finanziert?

Zu14.

Ziel des „EU Civil Society Empowerment Programme“ (CSEP), finanziert durch die EU Kommission, ist die Unterstützung der Zivilgesellschaft in allen Mitgliedstaaten bei der Verbreitung wirksamer und alternativer Diskurse im Internet. Weitere Informationen zum CSEP finden sich auch auf der Internetseite der Europäischen Kommission (exemplarisch: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en).

15. Auf welche Weise werden sich welche Internetunternehmen nach Kenntnis der Bundesregierung am CSEP beteiligen?

- a) Welche Ergebnisse zeitigte eine Auftaktveranstaltung des CSEP mit Internetfirmen und „Marketingexperten“ am 15. und 16. März 2017, nach der Kampagnen gestartet werden sollten*
- b) Auf welche Weise bzw. durch welche Maßnahmen könnte aus Sicht der Bundesregierung das Internet mit „positiven Narrativen“ gefüllt werden?*

Zu 15. und a)

Die Fragen 15 und 15a) werden zusammen beantwortet. Internetunternehmen haben auf dem 2. EU Internet Forum im Dezember 2016 ihre Bereitschaft zur Unterstützung des CSEP signalisiert. Die weitere Ausgestaltung der Beteiligung und Unterstützung wird von der EU Kommission ausgearbeitet. Informationen hinsichtlich der Ergebnisse zur Auftaktveranstaltung des CSEP liegen der Bundesregierung bislang nicht vor.

b)

Die Bundeszentrale für politische Bildung (BpB) leistet ihren Beitrag indem sie eine Vielzahl von Maßnahmen zur Stärkung der Medienkompetenz anbietet, die die Nutzer befähigen sollen das Internet selbstbestimmt, verantwortungsbewusst, kritisch und kreativ zu nutzen.

16. Wo sollen die CSEP-Trainings in Deutschland stattfinden, wer nimmt daran teil und welche Zielsetzung wird verfolgt (<http://gleift.de/1Ef>)?

Zu 16.

Informationen zu den CSEP-Trainings, die über die der oben genannten Internetseite hinausgehen, liegen der Bundesregierung nicht vor.

17. Was ist der Bundesregierung über den Fortgang des „e-evidence expert process“ bekannt, und welche Initiativen oder Maßnahmen werden dort zurzeit behandelt (Ratsdokument 10007/16)?

- a) Welche Initiativen hat die Bundesregierung im Rahmen des Prozesses ergriffen und welche Maßnahmen hat sie vorgeschlagen?
- b) Inwiefern wurde das Papier des Bundesministerium des Innern weiter behandelt, in dem vorgeschlagen wird die Europäische Ermittlungsanordnung in Strafsachen um eine Vorschrift zur „grenzüberschreitenden Sicherung elektronischer Daten ohne technische Hilfe“ zu ergänzen, und inwiefern sollte dies aus Sicht der Bundesregierung mit oder ohne eine Notifikation erfolgen?

Zu 17.

Die Europäische Kommission diskutiert in Umsetzung der Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ vom 9. Juni 2016 (Ratsdok. 10007/16) derzeit auf Fachebene mit Vertretern der Mitgliedstaaten Möglichkeiten zur Verbesserung der grenzüberschreitenden Gewinnung elektronischer Beweismittel zu Zwecken der Strafverfolgung. Eine Festlegung auf bestimmte Maßnahmen ist noch nicht erfolgt. Der Zwischenbericht der Europäischen Kommission vom 7. Dezember 2016 (Ratsdok. 15072/1/16) bietet unter Ziffer 3 einen Überblick über die zur Diskussion stehenden Optionen.

a)

Auf die Antwort der Bundesregierung zur Kleinen Anfrage der Fraktion DIE LINKE. zu Frage 2 auf Bundestagsdrucksache 18/10948 vom 23. Januar 2017, sowie zu Frage 13 auf Bundestagsdrucksache 18/11578 vom 20. März 2017 wird verwiesen.

b)

Der vom Bundesministerium der Justiz und für Verbraucherschutz koordinierte Regelungsvorschlag der Bundesregierung für eine Notifikationslösung für die direkte grenzüberschreitende Sicherung elektronischer Daten wurde als Beratungsgrundlage in die Fachgespräche zwischen Europäischer Kommission und Vertretern der Mitgliedstaaten eingebracht und in der Folge mit den Beteiligten diskutiert.

Nach dem Vorschlag soll der ermittelnde Mitgliedstaat dann zur Notifikation verpflichtet sein, wenn nicht ausgeschlossen werden kann, dass direkt zu sichernde Daten auf dem Territorium eines anderen Mitgliedstaates gespeichert sind.

18. Wann will die EU-Kommission ihre Prüfung beendet haben, inwiefern die Betreiber von Cloud-Diensten in den USA unter den Geltungsbereich der Europäischen Ermittlungsanordnung fallen könnten, wenn diese ihre Dienste in der Europäischen Union anbieten?

Zu 18.

Als nächsten Schritt hat die Europäische Kommission angekündigt, zum JI- Rat im Juni 2017 Optionen dazu zu unterbreiten, wie in den durch die Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ vom 9. Juni 2016 (Ratsdok. 10007/16) betroffenen Bereichen Verbesserungen bewirkt werden können, siehe hierzu auch die Antwort der Bundesregierung zu Frage 2 auf Bundestagsdrucksache 18/10948 vom 23. Januar 2017 sowie zu Frage 13c) auf Bundestagsdrucksache 18/11578 vom 20. März 2017.

19. Welche Fortschritte der sind der Bundesregierung zu der allgemeinen Debatte der Cybercrime-Konvention des Europarats zu der Frage bekannt, auch im Rahmen der Vereinten Nationen eine Cybercrime-Konvention zu erarbeiten (Drucksache 18/10591)?

Zu 19.

Auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/1059 vom 8. Dezember 2016 wird Bezug genommen. Es ist zu erwarten, dass die Debatte Gegenstand bei der Sitzung der Zwischenstaatlichen Expertengruppe Cybercrime (Intergovernmental Expert Group on Cybercrime - IEG Cybercrime) vom 10. bis 13. April 2017 in Wien sein wird. Die Haltung der Bundesregierung in dieser Frage ist unverändert.

20. Auf welche Weise ist das einjährige, von der Europäischen Kommission finanzierte „European Strategic Communication Network“ (ESCN) damit befasst, Mitgliedstaaten „anlassbezogen bei der strategischen Kommunikation im Rahmen der Bekämpfung des gewaltbereiten Extremismus“ zu beraten und welche Stellen werden dabei adressiert (Drucksache 18/10591)?

Zu 20.

Das European Strategic Communications Network (ESCN) berät einzelne Mitgliedstaaten beim Aufbau von Kapazitäten für den Bereich der strategischen Kommunikation im Rahmen der Bekämpfung des gewaltbereiten Extremismus.

Es wird auf Anfrage aus einem Mitgliedstaat tätig und adressiert staatliche Stellen, in der Regel auf Ebene der nationalen Regierungen, sowie Institutionen der EU. Darüber hinaus hat das ESCN ein Netzwerk der Mitgliedstaaten zum Informations- und Erfahrungsaustausch im Bereich der strategischen Kommunikation im Rahmen der Bekämpfung des gewaltbereiten Extremismus etabliert.

21. Auf welche Weise wollen Behörden der Bundesregierung (etwa die Bundeszentrale für politische Bildung oder das Bundeskriminalamt) ihre Zusammenarbeit im „Syria Strategic Communication Advisory Team“ (SSCAT) bzw. dessen Nachfolger The European Strategic Communications Network (ESCN) fortsetzen (Drucksache 18/10591)?

Zu 21.

Das Bundesministerium des Innern engagiert sich in dem in Antwort auf Frage 20 genannten vom ESCN etablierten Netzwerk der Mitgliedstaaten zum Informations- und Erfahrungsaustausch. In diesem Rahmen beteiligt sich das Bundesministerium des Innern derzeit an einem Analyseprojekt des ESCN zur Kommunikationsstrategie des sogenannten Islamischen Staats. Darüber hinaus besteht zwischen der BpB) und ESCN ein fachlicher Austausch im Rahmen von Expert/innen-Treffen. Das Auswärtige Amt tauscht sich zu Fragen der Auslandskommunikation mit dem ESCN aus.

22. Inwiefern sieht auch die Bundesregierung wie von den Agenturen Europol und Eurojust im Ratsdokument 7021/17 gefordert den Bedarf nach einer EU-weiten legislativen Regelung zur gemeinsamen Verwertung von einzelnen Regierungen erlangter Beweismittel („sharing of evidence“) oder der Durchführung gemeinsamer Ermittlungen im Internet („Online investigations“)?

Zu 22.

Es ist zu erwarten, dass die bis zum 22. Mai 2017 von den Mitgliedstaaten der EU umzusetzende Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen die grenzüberschreitende Kooperation innerhalb der EU sowohl im Hinblick auf den Austausch von Beweismitteln als auch für Ermittlungsmaßnahmen in einem online Kontext vereinfacht. Erst aufgrund der noch abzuwartenden praktischen Erfahrungen mit diesem neuen Kooperationsinstrument wird sich beurteilen lassen, ob Bedarf für weitere legislative Maßnahmen auf EU Ebene besteht.