



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](http://www.bmi.bund.de)

DATUM 21. Juni 2016

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

**Weitere europäische Anstrengungen zur möglichen Aushebelung  
verschlüsselter Telekommunikation**

**BT-Drucksache 18/8686**

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

Mit freundlichen Grüßen  
in Vertretung

Dr. Günter Krings

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.

Weitere europäische Anstrengungen zur möglichen Aushebelung verschlüsselter Telekommunikation

BT-Drucksache 18/8686

---

Vorbemerkung der Fragesteller:

Am 19. und 20. Mai 2016 führt die Polizeiagentur Europol eine Konferenz „Privacy in the digital age of encryption & anonymity online“ durch. Thematisiert wird die „Balance“ von Freiheit und Sicherheit. Nicht näher ausgeführte „Cyberkriminelle“ würden laut Europol Verfahren zur Verschlüsselung und Anonymisierung „aktiv missbrauchen“, um ihre Kommunikation und Identität zu verschleiern. Auch ihre Daten würden verschlüsselt gespeichert, außerdem nutzten sie virtuelle Währungen um ihre Finanztransaktionen zu verbergen. Die Konferenz geht der Frage nach, inwiefern dies als „Kollateralschaden“ von Freiheit toleriert werden kann oder ob Strafverfolgungsbehörden ähnlich wie bei früheren Kommunikationsformen Möglichkeiten zum Eindringen in die private Telekommunikation erhalten müssen.

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. Als weitere Hindernisse für Strafverfolger werden die „private Nutzung des Live-Streamings“, das Darknet und Anonymisierungswerkzeuge genannt. 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](http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf)). 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](http://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.



*Der im Herbst 2015 von Europol herausgegebene Lagebericht zu Cyberkriminalität thematisiert das Thema Verschlüsselung und Anonymisierung ausführlich (www.europol.europa.eu/content/internet-organisedcrime-threat-assessment-iocta-2015). In Ermittlungen würden jedoch in „zunehmendem Ausmaß“ digitalisierte Daten benötigt. Laut dem Europol-Direktor seien die Ermittlerinnen und Ermittler in drei Vierteln aller Fälle mit verschlüsselten Inhalten konfrontiert (https://twitter.com/rwainwright67/status/729229923982913536). Der Europol-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.*

*1. Auf welche Weise werden die im Ratsdokument 14369/15 dargestellten Herausforderungen hinsichtlich der Nutzung von verschlüsselungsbasierter Technologien in verschiedenen Kriminalitätsbereichen „mit Vorrang bearbeitet“ (Bundestagsdrucksache 18/7183)?*

Zu 1.

Die im Ratsdokument 14369/15 geschilderten Handlungsfelder werden im Rahmen der täglichen Arbeit der jeweils gesetzlich zuständigen Sicherheitsbehörden des Bundes berücksichtigt. Die Bundesregierung unterstützt darüber hinaus die weitere Bearbeitung der im Ratsdokument 14369/15 geschilderten Handlungsfelder in den Gremien der Europäischen Union, soweit diese dort auf der Tagesordnung stehen.

*2. Welche weiteren Arbeitsgruppen zu „terroristischen Online-Bedrohungen“ wurden nach Kenntnis der Bundesregierung einberufen und wer nahm daran teil (Bundestagsdrucksache 18/7183)?*

a) Mit welchem Ergebnis oder welchen Schlussfolgerungen haben die Arbeitsgruppen erörtert, „in welcher Weise Anonymisierung und Verschlüsselung die Bemühungen der Strafverfolgungsbehörden zur Ermittlung von Tätern und Tatverdächtigen erschweren und wie eine Zusammenarbeit mit der Privatwirtschaft insoweit hilfreich sein kann“?

b) Wo wurden die Ergebnisse oder Schlussfolgerungen der Arbeitsgruppe vorgestellt und / oder weiter beraten?

Zu 2., a) und b)

Die Fragen 2, 2 a) und 2 b) werden gemeinsam beantwortet. Der Bundesregierung sind keine weiteren Arbeitsgruppen zu „terroristischen Online Bedrohungen“ auf EU-Ebene bekannt. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 5, 5 a), 5 b), 5 c) der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 sowie auf die Antwort zu den Fragen 17 bis 19 der vorliegenden Kleinen Anfrage verwiesen.

*3. Wie werden die Ergebnisse einer bereits beendeten Arbeitsgruppe zu „terroristischen Online-Bedrohungen“ umgesetzt, deren in einem Abschlussbericht vorgeschlagenen Empfehlungen die Bundesregierung vorbehaltlos zustimmt (Bundestagsdrucksache 18/7183)?*

Zu 3.

Die von den Fragestellern genannte Arbeitsgruppe bestand nur zur Vorbereitung der „European Police Chiefs Convention“ am 23./24. September 2015 (s. Antwort der Bundesregierung zu den Fragen 5, 5 a), 5 b), 5 c) der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015). Die Ergebnisse der Arbeitsgruppe fließen in die tägliche Arbeit der jeweils gesetzlich zuständigen Sicherheitsbehörden des Bundes ein.

*4. Auf welche Weise hat sich nach Kenntnis der Bundesregierung die Gruppe „FoP Cyber“ seit Dezember 2015 mit dem Thema Verschlüsselung befasst?*

Zu 4.

In der Sitzung der Gruppe „Freunde der Präsidentschaft zu Cyber“ (FoP) am 1. Dezember 2015 wurde Verschlüsselung einerseits als wichtiger Schutz der Privatsphäre aber auch als Ursache erschwerter Beweissicherung im Strafverfahren diskutiert.

*5. Auf welche Weise haben der Europäische Auswärtige Dienst und die Europäische Verteidigungsagentur das Thema „Verschlüsselung der Kommunikationsinhalte sowie der Verschleierung der Identität“ nach Kenntnis der Bundesregierung in der jüngeren Vergangenheit behandelt (etwa im Rahmen der beschlossenen „Cyber-Diplomatie“ gegenüber Drittstaaten oder zur Umsetzung beschlossener Projekte zu „Cyber Defense“)?*



Zu 5.

Der Bundesregierung liegen keine Erkenntnisse vor, dass der Europäische Auswärtige Dienst (EAD) oder die European Defence Agency (EDA) in jüngerer Vergangenheit das Thema „Verschlüsselung der Kommunikationsinhalte sowie Verschleierung der Identität“ behandelt hätten. Auch die von den Fragestellern genannten Ratschlussfolgerungen Cyberdiplomatie behandeln das Thema nicht.

*6. In welchen polizeilichen Zusammenarbeitsformen auf Ebene der Europäischen Union (auch Ratsarbeitsgruppen) wurde nach Kenntnis der Bundesregierung thematisiert, den Zugang von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation durch den verstärkten Einsatz staatlich genutzter Trojanerprogramme zu ermöglichen?*

Zu 6.

Polizeiliche Zusammenarbeitsformen auf Ebene der Europäischen Union oder Ratsarbeitsgruppen, die sich mit dem „Zugang von Strafverfolgungsbehörden zu verschlüsselter Telekommunikation durch den verstärkten Einsatz staatlich genutzter Trojanerprogramme“ beschäftigen, sind der Bundesregierung nicht bekannt. Im Übrigen wird auf die Antwort zu den Fragen 29, 29a) und 29b) der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 verwiesen.

*7. Inwiefern würde die 2014 beschlossene EU-Richtlinie über die „Europäische Ermittlungsanordnung“ aus Sicht der Bundesregierung auch den grenzüberschreitenden Einsatz staatlich genutzter Trojanerprogramme umfassen (Bundestagsdrucksache 18/7707)?*

a) Wann will die Bundesregierung ihren Vorschlag zur Umsetzung der Richtlinie in das nationale Recht vorlegen? [BMJV]

b) Inwiefern ist von der Bundesregierung anvisiert, ausländischen Behörden dabei auch den grenzüberschreitenden Einsatz staatlich genutzter Trojanerprogramme zu ermöglichen?

Zu 7., a) und b)

Fragen 7, 7 a) 7 b) werden gemeinsam beantwortet. Die Bundesregierung beabsichtigt, ihren Vorschlag zur Umsetzung der Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen (RL EEA) noch in diesem Jahr und so rechtzeitig vorzulegen, dass die Umsetzungsfrist (22. Mai 2017) eingehalten werden kann.

Die RL EEA verfolgt das Ziel, die grenzüberschreitende Beweiserhebung in Strafverfahren innerhalb der EU zu vereinfachen und zu beschleunigen. Dazu sind z. B. standardisierte Formulare und Bearbeitungsfristen vorgesehen. Für die Frage, welche Ermittlungsmaßnahmen zur Erledigung einer EEA aus einem anderen Mitgliedstaat der Europäischen Union zur Verfügung stehen, bleibt grundsätzlich das Recht des ersuchten Mitgliedstaates maßgeblich.

Die zur Umsetzung der Richtlinie geplante Änderung des Gesetzes über die Internationale Rechtshilfe in Strafsachen (IRG) wird daher dem Grundsatz folgen, dass die deutschen Strafverfolgungsbehörden aufgrund eingehender EEAs nur solche Ermittlungsmaßnahmen ausführen können, die auch in einem entsprechenden deutschen innerstaatlichen Ermittlungsverfahren zur Verfügung stehen würden. Die Umsetzung der Richtlinie führt nicht zu einer Kompetenzerweiterung für deutsche Strafverfolgungsbehörden, was auch für den Einsatz von „Trojanerprogrammen“ gilt.

*8. In welchen Phänomen- und Kriminalitätsbereichen außer dem „Islamistischen Terrorismus“ nimmt das „Streben nach einer abgeschirmten, klandestinen Übermittlung von Informationen“ aus Sicht der Bundesregierung zu (Bundestagsdrucksache 18/5144)?*

Zu 8.

Nach Kenntnis der Bundesregierung findet sich ein Streben nach einer abgeschirmten, klandestinen Übermittlung von Informationen in allen Phänomenbereichen wieder, die von einem arbeitsteiligen, organisierten und vernetzten Zusammenwirken der Tatverdächtigen gekennzeichnet sind.

*9. Welche Techniken der „Verschlüsselung der Kommunikationsinhalte sowie der Verschleierung der Identität“ werden dabei bevorzugt angewandt?*



Zu 9.

Auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 wird verwiesen. Eine statistische Erfassung festgestellter Techniken der „Verschlüsselung der Kommunikationsinhalte sowie der Verschleierung der Identität“ erfolgt nicht.

*10. Inwiefern stehen deutsche Behörden wie von Europol geschildert ebenfalls vor dem Problem einer „zunehmenden privaten Nutzung des Live-Streaming“ durch mutmaßliche Straftäter (Ratsdokument 14369/15)?*

Zu 10.

Der Bundesregierung liegen im Hinblick auf eine zunehmende private Nutzung des Live-Streaming durch mutmaßliche Straftäter keine eigenen Erkenntnisse vor.

*11. In welcher Größenordnung sind deutsche Behörden nach Kenntnis der Bundesregierung mit verschlüsselten Inhalten konfrontiert (da hierüber keine Statistiken geführt werden, bitte nach „selten“, „häufig“ oder „sehr häufig“ kategorisieren)?*

Zu 11.

Auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 wird verwiesen. Für die Behörden des Bundes ist eine Kategorisierung in „selten“, „häufig“ oder „sehr häufig“ aufgrund fehlender statistischer Aufzeichnung nicht möglich.

*12. Über welche technischen Möglichkeiten für den „Zugriff auf Kommunikationsinhalte“ unter Umgehung oder Aushebelung von Verschlüsselung oder Anonymisierung sowie zur „Entschlüsselung der rechtmäßig abgefangenen Kommunikation“ verfügen die Polizeien und Geheimdienste des Bundes sowie die Zollkriminalämter derzeit (Bundestagsdrucksache 18/5144, bitte ungeachtet der jeweiligen gesetzlichen Grundlagen darstellen)?*

*a) Welche einzelnen „gängige[n] Werkzeuge“ wurden hierfür beschafft?*

*b) Sofern die Bundesregierung wie in der Bundestagsdrucksache 18/5144 abermals darauf verweist, dass Bundesbehörden über „keine universell einsatzbaren technischen Lösungen“ verfügen, welche einzelnen Verfahren kommen jeweils „nach dem Stand der Technik zum Einsatz“?*

Zu 12., a) und b)

Die Fragen 12, 12 a) und 12 b) werden gemeinsam beantwortet. Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung aber zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (BVerfGE 124, Seite 161, 189). Evident geheimhaltungsbedürftige Informationen muss die Bundesregierung nach der Rechtsprechung des Bundesverfassungsgerichts nicht offenlegen (BVerfGE 124, 161, 193 f.).

Die Abwägung kann dazu führen, dass die Bundesregierung nicht zur Arbeitsweise, Ausstattung und Methode der Sicherheitsbehörden Stellung nimmt. Ergibt die im Einzelfall vorzunehmende Abwägung, dass lediglich die Veröffentlichung einer geheimhaltungsbedürftigen Information ausgeschlossen ist, wird die Antwort unter Beachtung des jeweils erforderlichen Grades der Verschlussache bei der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Fragen 12, 12 a), 12 b) aus Geheimhaltungsgründen teilweise nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden können.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die teilweise Einstufung der Antwort auf die Fragen 12, 12 a), 12 b) als Verschlussache (VS) mit dem Geheimhaltungsgrad „VS – NUR FÜR DEN DIENSTGEBRAUCH“ ist aber im vorliegenden Fall erforderlich. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlussachen (Verschlussachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt würden.



Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Hinsichtlich der erbetenen Details insbesondere in Bezug auf den Bundesnachrichtendienst (BND) ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage nicht beantwortet werden kann. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren und daher in einer zur Veröffentlichung vorgesehenen Fassung nicht behandelt werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Bekanntgabe von Einzelheiten zu eingesetzten Methoden zur Aushebelung, Unbrauchbarmachung oder Umgehung von Verschlüsselungstechnik würde weitgehende Rückschlüsse auf die technischen Fähigkeiten und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential des BND zulassen. Dadurch könnte die Fähigkeit des BND, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des BND jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Derartige Erkenntnisse dienen insbesondere auch der Beurteilung der Sicherheitslage in den Einsatzgebieten der Bundeswehr im Ausland. Ohne dieses Material wäre eine solche Sicherheitsanalyse nur noch sehr eingeschränkt möglich, da das Sicherheitslagebild zu einem nicht unerheblichen Teil aufgrund von Informationen, die durch die technische Aufklärung gewonnen werden, erstellt wird. Das sonstige Informationsaufkommen des BND ist nicht ausreichend, um ein vollständiges Bild zu erhalten und Informationsdefizite im Bereich der technischen Aufklärung zu kompensieren.

Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten des BND bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten des BND gewinnen.

Dies würde folgeschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des BND - die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst) - 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 Entzifferung für die Aufgabenerfüllung des BND nicht ausreichend Rechnung tragen, 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 des BND so detailliert, 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 dem Geheimhaltungsinteresse des BND zurückstehen.

*13. Inwiefern hat die Summe der „individuellen Umstände und Rahmenbedingungen des jeweiligen Einsatzes“ von Technologien zur Umgehung, Aushebelung oder Unbrauchbarmachung von Verschlüsselung technische Defizite aufgezeigt, die bei Bundesbehörden einen Bedarf nach neuen Anwendungen oder Verfahren begründen könnten (Bundestagsdrucksache 18/5144)?*

#### Zu 13.

Die Sicherheitsbehörden des Bundes stehen vor der ständigen Aufgabe, mit dem technischen Fortschritt Schritt zu halten. Hierzu gehört auch, fortlaufend Bedarfe an neuen Anwendungen oder Verfahren zu identifizieren. Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 5 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/5144 vom 11. Juni 2015 verwiesen.



*14. Inwiefern stehen die Ermittlungsbehörden des Bundes weiterhin lediglich in „wenigen Einzelfällen“ vor dem Problem der Nutzung von „Anti-Forensik-Werkzeugen“, darunter Software zum Überschreiben von Inhalten oder Betriebssystemen, die von Wechselmedien gestartet werden?*

Zu 14.

Auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 wird verwiesen.

*15. Über welche Kenntnisse verfügt die Bundesregierung mittlerweile zur Umsetzung einer im „2015 Internet Organised Crime Threat Assessment“ (IOCTA) vorgetragenen Forderung von Europol, eine „zentrale Datenbank“ mit „VPN- und Proxy-Diensten“ anzulegen, und wo könnte diese angesiedelt werden (Bundestagsdrucksache 18/7183)?*

Zu 15.

Der Bundesregierung liegen hierzu keine weiteren Erkenntnisse vor. Auf die Antwort der Bundesregierung zu Frage 6 c) der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7183 vom 30. Dezember 2015 wird verwiesen.

*16. 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 (sofern möglich, bitte nach den Phänomenen „Islamistischer Terrorismus / Extremismus“, „Fluchthelfer“ und „hybride Bedrohungen“ differenzieren)?*

Zu 16.

Nach Kenntnis der Bundesregierung hat die European Internet Referral Unit (EU I-RU) bisher 178 Beiträge durch die Mitgliedsstaaten übermittelt bekommen (Stand 14. April 2016). Wie viele Internetinhalte infolgedessen von den jeweiligen Diensteanbietern aus dem Internet entfernt worden sind, ist der Bundesregierung nicht bekannt.

Im Übrigen wird auf die Antwort der Bundesregierung zu Fragen 1 bis 4 der Kleinen Anfrage „Gemeinsame Meldeplattform der Internetbranche und Europol“ der Fraktion DIE LINKE. zu Bundestagsdrucksache 18/8670 die dem Deutschen Bundestag am 17. Juni 2016 übermittelt wurde (BT-Drs. neu liegt noch nicht vor) wird verwiesen. Der Bundesregierung liegen keine darüber hinausgehenden Erkenntnisse vor.

*17. Bei welchen Treffen oder einem sonstigen Austausch des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister“ bzw. entsprechenden Unterarbeitsgruppen wurde das Thema Verschlüsselung nach Kenntnis der Bundesregierung behandelt, und wer trug dazu vor?*

Zu 17.

Im Rahmen des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister“ wurde das Thema Verschlüsselung nach Kenntnis der Bundesregierung bislang nicht inhaltlich behandelt. Im Übrigen wird auf die Antwort der Bundesregierung auf die Mündliche Frage 17 des Abgeordneten Andrej Hunko, Anlage 16 zum Plenarprotokoll 18/142 der Fragestunde im Deutschen Bundestag am 2. Dezember 2015, verwiesen.

*18. Was ist der Bundesregierung darüber bekannt, auf welchen zukünftigen Treffen das Thema Verschlüsselung behandelt werden soll?*

Zu 18.

Der Bundesregierung ist nicht bekannt, auf welchen zukünftigen Treffen des „Forums der Internetdienstleister“ das Thema Verschlüsselung behandelt werden soll.

*19. Was ist der Bundesregierung mittlerweile 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 (Bundestagsdrucksache 18/7183)?*

Zu 19.

Auf die Antwort der Bundesregierung zu Frage 24 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/ 7183 vom 30. Dezember 2015 wird verwiesen. Der Bundesregierung liegen keine darüber hinausgehenden Erkenntnisse vor.



*20. Welche Schlussfolgerungen zieht die Bundesregierung aus den Diskussionen der Europol-Konferenz „Privacy in the digital age of encryption & anonmity online“ über die „Balance“ von Freiheit und Sicherheit hinsichtlich der Frage, ob es eher an Freiheit oder eher an Sicherheit fehlt, es also weiterer oder keiner weiteren Möglichkeiten des Zugangs von Strafverfolgungsbehörden zu verschlüsselten Kommunikationsinhalten oder verschleierte Identitäten bedarf?*

Zu 20.

Nach Auffassung der Bundesregierung sind Freiheit und Sicherheit nicht als Gegensatz zu verstehen. Deshalb hat die Bundesregierung aus den Diskussionen der Europol-Konferenz „Privacy in the digital age of encryption & anonmity online“ keine der Fragestellung entsprechenden Schlussfolgerungen gezogen. Zur Haltung der Bundesregierung im Hinblick auf Verschlüsselung wird auf die Antwort der Bundesregierung auf die Schriftliche Frage des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 18/6760, Nr. 21 vom 20. November 2015 verwiesen.