Deutscher Bundestag **Drucksache 18/8686**

18. Wahlperiode 31.05.2016

Kleine Anfrage

der Abgeordneten Andrej Hunko, Frank Tempel, Annette Groth, Dr. André Hahn, Inge Höger, Ulla Jelpke, Jan Korte, Niema Movassat, Harald Petzold (Havelland), Dr. Petra Sitte, Alexander Ulrich und der Fraktion DIE LINKE.

Weitere europäische Anstrengungen zur möglichen Aushebelung verschlüsselter Telekommunikation

Am 19. und 20. Mai 2016 führt die Polizeiagentur Europol eine Konferenz „Privacy in the digital age of encryption & anonmity 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 EU-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). 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.

Der im Herbst 2015 von Europol herausgegebene Lagebericht zu Cyberkriminalität thematisiert das Thema der 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.

Wir fragen die Bundesregierung:

1. Auf welche Weise werden die im Ratsdokument 14369/15 dargestellten Herausforderungen hinsichtlich der Nutzung von verschlüsselungsbasierten Technologien in verschiedenen Kriminalitätsbereichen „mit Vorrang bearbeitet“ (Bundestagsdrucksache 18/7183)?
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?
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)?
4. Auf welche Weise hat sich nach Kenntnis der Bundesregierung die Gruppe „FoP Cyber“ seit Dezember 2015 mit dem Thema der Verschlüsselung befasst?
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“)?
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?
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?
   b) Inwiefern ist von der Bundesregierung anvisiert, ausländischen Behörden dabei auch den grenzüberschreitenden Einsatz staatlich genutzter Trojanerprogramme zu ermöglichen?
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)?

9. Welche Techniken der „Verschlüsselung der Kommunikationsinhalte sowie der Verschleierung der Identität“ werden dabei bevorzugt angewandt?
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)?
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)?
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 auf 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“?
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)?
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?
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)?
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)?
17. Bei welchen Treffen oder welchem sonstigen Austausch des am 3. Dezember 2015 gestarteten „Forums der Internetdienstleister“ bzw. entsprechender Unterarbeitsgruppen wurde das Thema der Verschlüsselung nach Kenntnis der Bundesregierung behandelt, und wer trug dazu vor?
18. Was ist der Bundesregierung darüber bekannt, auf welchen zukünftigen Treffen das Thema der 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)?

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 verschleierten Identitäten bedarf?

Berlin, den 30. Mai 2016

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