Deutscher Bundestag **Drucksache 19/16427**

19. Wahlperiode 09.01.2020

Kleine Anfrage

der Abgeordneten Andrej Hunko, Martina Renner, Heike Hänsel, Ulla Jelpke, Niema Movassat, Zaklin Nastic, Thomas Nord, Alexander Ulrich und der Fraktion DIE LINKE.

Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen im zweiten Halbjahr 2019

Halbjährlich fragen die Abgeordneten der Fraktion DIE LINKE. beim Bundesministerium des Innern, für Bau und Heimat, beim Bundesministerium der Finanzen und beim Bundeskanzleramt nach den Zahlen von Einsätzen digitaler Fahndungsmethoden (Bundestagsdrucksachen 19/7104, 19/3678, 19/505, 18/11041, 18/4130, 18/2257, 18/5645, 18/7285, 18/9366, 18/11041). Hintergrund ist die zunehmende Überwachung und Analyse digitaler Verkehre, die das Vertrauen in die Freiheit des Internet und der Telekommunikation untergraben. Aus Antworten aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz „Stiller SMS“, sogenannter „WLAN-Catcher“ und „IMSI-Catcher“ nimmt zu. Aus Sicht der Fragestellerinnen und Fragesteller sind diese Maßnahmen mitunter rechtlich gar nicht gestattet, etwa der Einsatz „Stiller SMS“. Denn Polizei und Geheimdienste dürfen nur passiv die Kommunikation von Telefonen abhören, die „Stillen SMS“ werden aber von den Behörden erst erzeugt.

Während die Bundesregierung zwar Angaben zu „Stillen SMS“ des Bundeskriminalamtes und der Bundespolizei macht, bleiben Zahlen für den Zoll seit 2012 als Verschlusssache eingestuft. Hinsichtlich des Bundesnachrichtendienstes unterbleibt jede Mitteilung. Mit Beantwortung der Drucksache 19/7847 ging das Bundesministerium des Innern, für Bau und Heimat dazu über, ab 2019 auch die Zahlen zu „Stillen SMS“ des Bundesamtes für Verfassungsschutz (BfV) als „VS – Geheim“ einzustufen. Diese seien besonders schutzbedürftig, da sich „durch die regelmäßige halbjährliche Beantwortung […] Einzelinformationen zu einem umfassenden Lagebild verdichten können“. Die halbjährlichen Abfragen führten zu solch einer „Verdichtung“, auf diese Weise könnten Rückschlüsse auf die „technischen Fähigkeiten“ des Inlandsgeheimdienstes gezogen werden (vgl. Schreiben des Parlamentarischen Staatssekretärs Günter Krings an den MdB Andrej Hunko vom 11. März 2019).

Die Wissenschaftlichen Dienste des Deutschen Bundestages betonen hingegen, dass derartige Beschränkungen dem verfassungsrechtlichen Verhältnismäßigkeitsgebot unterliegen (WD 3 – 3000 – 121/19). Die Bundesregierung muss demnach mildere, gleich geeignete Mitteln suchen, anstatt die vorher offen mitgeteilten Informationen nunmehr als „VS – Geheim“ einzustufen. Auch die Verschlusssachenanweisung (VSA) bestimmt in § 15 S. 3, dass ein geringerer Einstufungsgrad oder ein anderes, einer Geheimhaltung gleich geeignetes Mittel Vorrang haben muss. So ließen sich den Wissenschaftlichen Diensten zufol-

ge Informationen dergestalt abstrahieren, dass auf geschützte Interessen des Staates keine wesentlichen Rückschlüsse mehr möglich sind. Im Ergebnis könnten dem Bundestag so z. B. abstrakte Informationen offen übermittelt werden sowie zugleich in der Geheimschutzstelle des Bundestages konkretere, aber eingestufte Informationen.

Wir fragen die Bundesregierung:

1. Wie oft haben welche Bundesbehörden im zweiten Halbjahr 2019 von „WLAN-Catchern“ Gebrauch gemacht?
   a) Welche Bundesbehörden haben zwar selbst keine „WLAN-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?
   b) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
   c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
   d) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?
   e) Welche Hard- und Software wird für die „WLAN-Catcher“ genutzt, bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben?
   f) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?
2. Welche Bundesbehörden haben im zweiten Halbjahr 2019 wie oft „IMSI-Catcher“ eingesetzt?
   a) Welche Bundesbehörden haben zwar selbst keine „IMSI-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?
   b) Welche Hard- und Software wird für die „IMSI-Catcher“ genutzt?
   c) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
   d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
   e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?
   f) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?
   g) Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung im zweiten Halbjahr 2019 Ausfuhrgenehmigungen für sogenannte IMSI-Catcher in welche Bestimmungsländer erteilt?
   h) Wie viele IMSI-Catcher bzw. ähnliche Abhöranlagen für den Mobilfunkverkehr haben das Bundesamt für Sicherheit in der Informationstechnik oder andere zuständige Bundesbehörden (auch in deren Auftrag) im zweiten Halbjahr 2019 im Regierungsviertel oder in räumlicher Nähe

anderer Bundesbehörden aufgespürt, und welche Betreiber der Anlagen wurden ausfindig gemacht?

3. Welche Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone sogenannte „Stille SMS“ zum Ausforschen des Standortes ihrer Besitzerinnen und Besitzer oder dem Erstellen von Bewegungsprofilen zu verschicken, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

   a) Welche Bundesbehörden haben zwar selbst keine „Stillen SMS“ eingesetzt, sich hierfür aber anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?

   b) Wie viele „Stille SMS“ wurden von den jeweiligen Behörden im zweiten Halbjahr 2019 bzw. in deren Auftrag durch andere Behörden oder Firmen insgesamt jeweils versandt (bitte bezüglich des Zollkriminalamts nach den einzelnen Zollfahndungsämtern aufschlüsseln)?

   c) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?

   d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?

   e) Ist die Bundesregierung, sofern sie die Zahlen zu „Stillen SMS“ des BfV weiterhin als „VS – Geheim“ einstuft, bereit, dem Bundestag wenigstens abstrahierte Informationen hierzu offen zu übermitteln und zugleich in der Geheimschutzstelle des Bundestages konkretere, aber eingestufte Informationen zu hinterlegen?

   f) Welche Hard- und Software wird von den Behörden zum Versand und zur Auswertung von „Stillen SMS“ genutzt, bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben (Bundestagsdrucksache 18/7285)?

4. Wie viele Maßnahmen der Funkzellenauswertung haben welche Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 vorgenommen (bitte wie auf Bundestagsdrucksache 17/14714 beantworten)?

   a) Welche Bundesbehörden haben zwar selbst keine Maßnahmen der Funkzellenauswertung eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?

   b) Wie viele Anschlüsse, Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen?

   c) Welche der Funkzellenabfragen wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof gestattet, und im Zusammenhang mit welchen Ermittlungen fanden diese statt?

   d) Wie viele Betroffene sind über die Maßnahmen nachträglich benachrichtigt worden (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

   e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?

f) Inwiefern haben die Maßnahmen aus dem ersten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

5. In welchem Umfang haben Bundesbehörden im zweiten Halbjahr 2019 geolokalisierte Standortdaten von Mobiltelefonen bei Herstellern der Geräte bzw. der Betriebssysteme abgefragt (bitte für BKA, Bundespolizei, BfV, Zollkriminalamt darstellen)?

6. Inwiefern sind Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr mittlerweile in der Lage, Mikrofone von Mobiltelefonen aus der Ferne zu aktivieren, um diese als Abhöreinrichtungen zu nutzen, in welchem Umfang wird dies bereits genutzt, und welche Soft- oder Hardware wird hierfür genutzt, bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

7. Wie oft haben Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 Trojaner-Programme bzw. ähnliche Überwachungssoftware eingesetzt oder einsetzen lassen (bitte jeweils nach Polizei, Zoll, Geheimdiensten aufschlüsseln)?

   a) Welche der verfügbaren Programme (etwa „Übergangslösung“, Trojaner zur „Online-Durchsuchung“, Trojaner zur „Quellen-TKÜ“) kamen dabei jeweils zur Anwendung?

   b) In welchem Umfang haben Bundesbehörden im vergangenen Halbjahr Trojaner auf mobilen Geräten platziert?

   c) Wie viele Personen und Ermittlungsverfahren waren von den Einsätzen der Trojaner insgesamt betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

   d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?

   e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

8. In welchem Umfang haben die Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 die Möglichkeit genutzt, sich Zugang auf Nutzeraccounts bei den Messengerdiensten Signal, WhatsApp, Telegram oder vergleichbaren Anwendungen zu verschaffen, indem sich Ermittlerinnen oder Ermittler dort mit einem weiteren Gerät zum Mitlesen einloggen?

9. Worin unterscheidet sich eine „Vordertür“ („Frontdoor“), wie sie der Präsident des Bundeskriminalamtes zum staatlichen Zugang zu verschlüsselter Ende-zu-Ende-Telekommunikation ins Gespräch bringt („Crypto Wars: BKA-Chef will ‚Frontdoor-Debatte‘ führen“, www.heise.de vom 23. November 2019), von einer „Hintertür“ („Backdoor“), mit der die Betreiber zur „Herausgabe einer unkryptierten Überwachungskopie“ verpflichtet werden könnten (bitte die technischen und rechtlichen Unterschiede erläutern; vgl. auch „Interpol group delays criticism of encryption after objections“, Reuters vom 27. November 2019), und welche politischen Initiativen auf Ebene der Europäischen Union sind der Bundesregierung wie vom BKA-Präsidenten erwähnt zu einer solchen „Frontdoor-Debatte“ bekannt?

10. Mit welchen Anfragen hat sich das BKA in der Vergangenheit an die „Entschlüsselungsplattform“ bei Europol gewandt bzw. Unterstützung erfolgte von der Abteilung in Ermittlungsverfahren (Antwort zu Frage 8 auf Bundestagsdrucksache 19/15658)?

    a) Welche Geräte (etwa Speichermedien, Rechner, Telefone), Anwendungen (Software oder Apps) oder Verfahren können von der „Entschlüsselungsplattform“ entschlüsselt werden?

    b) Seit wann hat die „Entschlüsselungsplattform“ mit diesen Unterstützungsmaßnahmen begonnen, und wie häufig wird sie vom BKA angefragt?

11. Welche Soft- und Hardware haben das Bundesministerium der Verteidigung, das Bundeskanzleramt oder dem Bundesministerium des Innern, für Bau und Heimat nachgeordnete Sicherheitsbehörden für die Überwachung öffentlich zugänglicher Quellen und geschlossener Foren im Internet beschafft, bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12465 ergeben?

12. Welche „Methoden der Computerlinguistik und der Künstlichen Intelligenz“ haben das Bundesministerium der Verteidigung, das Bundeskanzleramt oder dem Bundesministerium des Innern, für Bau und Heimat nachgeordnete Sicherheitsbehörden im zweiten Halbjahr 2019 zum Abgleich genutzt, bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12465 ergeben?

13. Welche „Methoden des maschinellen Lernens“ wurden im Bundeskriminalamt im zweiten Halbjahr 2019 „im Einzelfall anlassbezogen“ auf Datenbestände von Ermittlungsverfahren angewendet, bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12465 ergeben?

Berlin, den 17. Dezember 2019

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