

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, Wolfgang Gehrcke, Ulla Jelpke, Niema Movassat, Dr. Alexander S. Neu, Martina Renner, Dr. Petra Sitte, Kersten Steinke, Halina Wawzyniak, Jörn Wunderlich und der Fraktion DIE LINKE.

Einsätze von so genannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2015

Berichte über die zunehmende Überwachung und Analyse digitaler Verkehre untergraben das Vertrauen in die Freiheit des Internets und der Telekommunikation. Aus Antworten aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz „stiller SMS“, so genannter WLAN-Catcher und IMSI-Catcher nimmt stetig zu, die Ausgaben für Analysesoftware steigen ebenfalls (Bundestagsdrucksachen 18/4130, 18/2257). Das Bundeskriminalamt hat zwei verschiedene Trojaner entwickelt und nutzt zeitgleich eine „Übergangslösung“. Der Trojaner zur „Online-Durchsuchung“ kompletter Rechnersysteme sei „einsatzbereit“ (Schriftliche Fragen 22 und 23 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/2352). Ein weiteres System zum ferngesteuerten Abhören von verschlüsselter Internettelefonie werde noch erprobt. Damit verfügt die Behörde über mindestens drei verschiedene Trojaner. Auch die Fähigkeiten zur Bildersuche in Polizeidatenbanken werden weiterentwickelt; beispielsweise nutzt das Bundeskriminalamt immer häufiger die Möglichkeit der Abfrage seiner Datenbestände mittels Aufnahmen aus Überwachungskameras.

Wir fragen die Bundesregierung:

1. Wie oft haben welche Bundesbehörden im ersten Halbjahr 2015 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 nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - d) Welche Hard- und Software wird hierfür genutzt, und welche Änderungen haben sich hierzu gegenüber dem Jahr 2014 ergeben (Bundestagsdrucksachen 17/14714, 18/2257, 18/4130)?
 - e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

2. Welche Bundesbehörden haben im ersten Halbjahr 2015 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) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?
 - e) Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung im ersten Halbjahr 2015 Ausführgenehmigungen für so genannte IMSI-Catcher in welche Bestimmungsländer erteilt?
3. Wie hat sich die Zahl der vom Bundesamt für Sicherheit in der Informationstechnik oder von anderen zuständigen Bundesbehörden (auch in deren Auftrag) aufgespürten IMSI-Catcher bzw. ähnlichen Abhöranlagen für den Mobilfunkverkehr im Regierungsviertel oder in räumlicher Nähe anderer Bundesbehörden seit dem Jahr 2010 entwickelt, und in welchen Fällen konnten die Betreiber der Anlagen durch Bundesbehörden ausfindig gemacht werden (bitte diese Verantwortlichen jeweils benennen)?
4. Welche Bundesbehörden sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone „stille SMS“ zum Ausforschen des Standortes ihrer Besitzerinnen und Besitzer oder dem Erstellen von Bewegungsprofilen zu verschicken, bzw. welche Änderungen haben sich gegenüber dem zweiten Halbjahr 2014 ergeben?
 - a) Welche Bundesbehörden haben zwar selbst keine „stillen SMS“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?
 - b) Wie viele „stille SMS“ haben diese Behörden in den letzten fünf Jahren durch andere Behörden versenden lassen (bitte nach Halbjahren darstellen)?
 - c) Wie viele „stille SMS“ wurden von den jeweiligen Behörden im ersten Halbjahr 2015 bzw. in deren Auftrag durch andere Behörden oder Firmen insgesamt jeweils versandt (bitte bezüglich des Zollkriminalamts nach den einzelnen Zollfahndungsämtern aufschlüsseln)?
 - d) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - e) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - f) Welche Hard- und Software wird hierfür genutzt, und welche Änderungen haben sich hierzu gegenüber dem Jahr 2014 ergeben (Bundestagsdrucksache 18/2257)?
 - g) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

5. Wie viele Maßnahmen der Funkzellenauswertung haben welche Bundesbehörden im ersten Halbjahr 2015 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) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden (bitte nach Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - d) Welche Funkzellenabfragen wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof gestattet, und im Zusammenhang mit welchen Ermittlungen fanden diese statt?
 - e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?
6. Inwiefern sind Bundesbehörden des Innern, der Verteidigung, der Finanzen oder des Bundeskanzleramtes 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 zweiten Halbjahr 2014 ergeben?
7. Welche weiteren Hersteller haben im ersten Halbjahr 2015 an polizeiliche oder geheimdienstliche Bundesbehörden Software zur computergestützten Bildersuche bzw. zu Bildervergleichen (auch testweise) geliefert, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, bzw. welche Nutzung ist anvisiert, welche konkreten Behörden bzw. deren Abteilungen sind bzw. wären darüber zugriffsberechtigt, in welchen Ermittlungen kommen bzw. kämen diese im Einzel- oder Regelfall zur Anwendung, bzw. welche Änderungen haben sich gegenüber dem zweiten Halbjahr 2014 ergeben?
 - a) Welche Kosten sind für Tests oder Beschaffung entsprechender Software entstanden?
 - b) Auf welche Datensätze kann die etwaige, neu beschaffte Software zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, und welche konkreten Behörden bzw. deren Abteilungen sind darüber zugriffsberechtigt?
 - c) Inwiefern kann die Bundesregierung mitteilen, ob die Anwendung von Software zur computergestützten Bildersuche bzw. zu Bildervergleichen im Vergleich zum Jahr 2014 zu- oder abnimmt?
 - d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen, bzw. inwiefern lässt sich dies überhaupt rekonstruieren?

8. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung (bitte nach Vorgangsbearbeitung, kriminalistischer Fallbearbeitung aufschlüsseln), bzw. welche Änderungen haben sich gegenüber dem zweiten Halbjahr 2014 ergeben?
 - a) Welche Kosten sind Bundesbehörden im Einzelfall und unter Berücksichtigung der Arbeitszeit innerhalb der Behörde für die Beschaffung, Anpassung, den Service und die Pflege der Software im ersten Halbjahr 2015 entstanden?
 - b) Welche weiteren Produkte der Firma rola Security Solutions GmbH (auch „Zusatzmodule“) wurden für welche Behörden und welche Einsatzzwecke beschafft, bzw. welche Änderungen haben sich gegenüber dem zweiten Halbjahr 2014 ergeben?
 - c) Inwiefern und wofür werden Anwendungen von rola Security Solutions auch bei In- und Auslandsgeheimdiensten der Bundesregierung genutzt, bzw. welche Änderungen haben sich gegenüber dem zweiten Halbjahr 2014 ergeben?
9. Inwiefern und auf welche Weise wird der Internetknoten DE-CIX bzw. werden andere in Deutschland oder auch im Ausland befindliche, internationale Schnittstellen von Glasfaserkabeln durch welche Bundesbehörden überwacht, bzw. welche Änderungen haben sich hierzu ergeben (Bundestagsdrucksachen 17/14714, 18/2257, 18/4130)?
10. Wie oft haben welche Bundesbehörden im ersten Halbjahr 2015 Trojaner-Programme bzw. sonstige beim CC ITÜ vorgehaltene Überwachungssoftware eingesetzt oder einsetzen lassen?
 - a) Welche der verfügbaren Programme (etwa „Übergangslösung“, Trojaner zur „Online-Durchsuchung“, Trojaner zur „Quellen-TKÜ“, TKÜ – Telekommunikationsüberwachung) kam dabei jeweils zur Anwendung?
 - b) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?
 - c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

Berlin, den 2. Juni 2015

Dr. Gregor Gysi und Fraktion