

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, Dr. André Hahn, Inge Höger, Ulla Jelpke, Dr. Petra Sitte, Frank Tempel, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.

Neue digitale Überwachungsmethoden

Die Polizeien und Geheimdienste des Bundes verfügen über technische Werkzeuge (Hardware, Software) zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten (Bundestagsdrucksache 17/12651). Hersteller und Funktionalität der Produkte sind vielfach unbekannt. Mitgeteilt wird häufig lediglich, es würden „handelsübliche wie auch eigenentwickelte Hard- und Software“ genutzt. Auch für neuere Internetdienste (etwa Cloud-Verfahren) werden Verfahren zum Abhören von Metadaten oder Mitlesen von Inhalten entwickelt (Plenarprotokoll 17/210). Die rechtliche Grundlage ist dabei vielfach unklar und bezieht sich auf Gesetze, die lange vor der Einführung der neuen Dienste erlassen wurden. Dies gilt ebenso für neuere, digitale Ortungsverfahren, wie etwa von Mobiltelefonen. Im Bundesministerium des Innern (BMI) existieren deshalb immer wieder Arbeitsgruppen, die rechtliche Rahmenbedingungen erörtern sollen. Die Rede ist von „organisatorischen und personellen Herausforderungen, die sich aus den Entwicklungen auf dem Gebiet der Telekommunikation für die Sicherheitsbehörden ergeben“ (Bundestagsdrucksache 18/2257). Im BMI ist hierzu ein „Runder Tisch zur Sicherstellung der Telekommunikationsüberwachung in der Zukunft“ eingerichtet worden.

Wir fragen die Bundesregierung:

1. Über welche technischen Werkzeuge (Hardware, Software) verfügen welche Bundesbehörden zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten, bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 17/12651 ergeben?
2. Welche „kommerziell verfügbare[n] Softwarewerkzeuge“ werden hierfür im Bundeskriminalamt (BKA) eingesetzt?
3. Welche „handelsübliche wie auch eigenentwickelte Hard- und Software“ wird vom Bundesnachrichtendienst (BND) und vom Bundesamt für Verfassungsschutz (BfV) „zur Entzifferung“ eingesetzt (bitte die Hersteller sowie die weiteren Beteiligten der „Eigenentwicklungen“ benennen)?
4. Inwiefern hält die Bundesregierung Möglichkeiten für Behörden des BMI zum Knacken oder Umgehen von Verschlüsselung für unabdingbar oder entbehrlich?

5. In wie vielen Fällen war eine Verschlüsselung nach Einschätzung der Bundesregierung hinderlich bei der Ermittlung, bzw. in wie vielen Fällen hat eine nachträgliche Entschlüsselung wesentlich zur Aufklärung von Tatkomplexen beigetragen?
6. Inwiefern trifft es zu, dass der BND in Afghanistan, Somalia und/oder dem Nahen Osten „jegliche Art von Kommunikation“ abhört und speichert und hiermit „Telefonie, Internetnutzung, E-Mail, GPS-Datenverarbeitung etc.“ gemeint ist (DER SPIEGEL, 8. September 2014)?
7. Welche weiteren Länder wurden auf diese Weise in den Jahren 2013 und 2014 von der ehemaligen Echelon-Station Bad Aibling in Bayern abgehört?
8. Inwiefern hat die Bundesregierung gegenüber den USA versucht zu klären, ob Berichte zutreffen, wonach sich der Militärgheimdienst NSA Zugriff auf deutsche Internetnetzwerke verschafft hat, wozu laut einem Dokument des Whistleblowers Edward Snowden die Telekom Deutschland GmbH und der Kölner Provider NetCologne Gesellschaft für Telekommunikation mbH gehören (SPIEGEL ONLINE, 17. September 2014)?
 - a) Sollten diese Berichte zutreffen, welcher Straftat hätten sich die USA in diesem Falle schuldig gemacht?
 - b) Sofern die Bundesregierung hierzu gegenüber den USA nicht tätig wurde, auf welche Weise wird sie diesem Verdacht einer möglichen Straftat nachgehen?
9. Welche neueren Details kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung sowie einer „Verschlüsselung im Bereich des Cloud-Computing im Allgemeinen“ beschäftigt (Plenarprotokoll 17/210)?
 - a) Welche „fachliche[n] Fragestellungen“ wurden vom BKA, der Bundespolizei oder dem BfV im Rahmen des Projekts „CLOUD“ formuliert (Bundestagsdrucksache 17/12651)?
 - b) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen erbringen welche Leistungen für das Projekt?
10. Welche wesentlichen (Zwischen-)Ergebnisse kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, und welche Schlussfolgerungen zieht sie daraus?
 - a) Welche „potentiellen technischen Möglichkeiten für einen Zugriff der Sicherheitsbehörden“ wurden identifiziert?
 - b) Welche „rechtlichen Rahmenbedingungen“ wurden erörtert?
 - c) Inwiefern hält die Bundesregierung technische Möglichkeiten zum Knacken der Passwörter von Cloud-Diensten zur Strafverfolgung als von der Strafprozessordnung gedeckt?
11. Von welchen Möglichkeiten zur Überwachung bzw. der Rekonstruktion der Nutzung von digitalen Kopiergeräten haben Bundesbehörden bereits Gebrauch gemacht?
 - a) Was ist der Bundesregierung darüber bekannt, inwiefern digitale Kopierer über technische Möglichkeiten zum automatisierten Aufspüren kopierter Banknoten oder andere Wertpapiere verfügen?
 - b) Inwiefern und nach welchem Verfahren werden welche Bundesbehörden von Herstellern oder Aufstellern von Stand-alone-Kopierern oder netz-angebundenen Kopierern benachrichtigt, wenn mit diesen Banknoten oder andere Wertpapiere vervielfältigt werden?

- c) Welche Bundesbehörden nutzen für polizeiliche oder geheimdienstliche Zwecke in Kopien verborgene Kennzeichen der Kopierer, und um welche technischen Verfahren handelt es sich dabei?
12. Worum handelt es sich bei den an die Firma ELETTRONICA GmbH vergebenen Aufträge „Ausbau von drei kriminalpolizeilichen Spezialfahrzeugen für das Bundeskriminalamt“ sowie „Ausbau von zwei Fahrzeugen für die Bundespolizei“ (Bundestagsdrucksache 18/2292)?
13. Welche Überwachungstechnik welcher Firmen ist in den Fahrzeugen verbaut?
14. Worum handelte es sich bei der Lieferung einer „Nachbearbeitungsplattform Strix“ für das BKA durch die Firmen MEDAV GmbH und/oder Vedit Systems GmbH (Bundestagsdrucksache 18/2292)?
15. Welche Fragestellungen bzw. technischen Lösungen hat das „Forschungsprojekt zur prototypischen Realisierung einer Verarbeitungsplattform für Daten aus Telekommunikationsüberwachungen“ mit der Firma MEDAV GmbH untersucht (Bundestagsdrucksache 18/2292)?
- a) Welche weiteren Partner erhielten welche weiteren Aufträge?
- b) Welche Ergebnisse zeitigte das Projekt, und welche Schlussfolgerungen zieht die Bundesregierung daraus?
16. Welche Studien oder Projekte zur Überwachung (nicht Ortung) von Smartphones haben Behörden des BMI, des Bundesministeriums der Verteidigung oder des Bundeskanzleramtes in den vergangenen fünf Jahren durchgeführt bzw. deren Ergebnisse angefordert (um einen Überblick über etwaige grundrechtsrelevante Verfahren zu bekommen, bitte die Zielsetzung der Studien oder Projekte kurz schildern), und wer sind die Auftragnehmer oder Unterauftragnehmer jener Studien oder Projekte?
17. Welche Fragestellungen bzw. technischen Lösungen hat das Forschungsprojekt „Mehrwegepeiler und Systemdemonstrator“ der Firma MEDAV GmbH im Rahmen des Verbundvorhabens „Emitter Identifikation und Lokalisierung unter Mehrwegeausbreitungsbedingungen“ (EILT) untersucht (Bundestagsdrucksache 18/2292)?
- a) Welche technischen Verfahren zur Ausbreitung von Funksignalen bzw. deren Präzisions-Lokalisierungen wurden dabei genau untersucht?
- b) Welche weiteren Partner erhielten welche weiteren Aufträge?
- c) Welche Ergebnisse zeitigte das Projekt, und welche Schlussfolgerungen zieht die Bundesregierung daraus?
18. Welche weiteren technischen Möglichkeiten oder Protokolle (außer IMSI-Catchern) werden von welchen Bundesbehörden zur Ortung von Mobiltelefonen bzw. einer Eingrenzung von deren Standort angewandt?
19. Inwiefern haben sich die Bundesbehörden des Innern, der Verteidigung oder das Bundeskanzleramt bereits mit dem Aufbau eigener Fähigkeiten zur Ortung von Mobiltelefonen durch das „Signalling System #7“ (Signalisierungssystem Nummer 7; SS7) befasst (Netzpolitik, 26. August 2014)?
- a) Welche Behörden, Institute oder Firmen haben hierfür welche Aufträge erhalten, und welche Verfahren wurden untersucht?
- b) Welche Bundesbehörden verfügen zu welchem Zweck über wie viele SS7-Zugänge?
- c) Inwiefern haben sich die Bundesbehörden des Innern, der Verteidigung oder das Bundeskanzleramt bereits mit der Abwehr oder Verhinderung einer Ortung von Mobiltelefonen durch das SS7 befasst?

- d) Welche Behörden, Institute oder Firmen haben hierfür welche Aufträge erhalten, und welche Verfahren wurden untersucht?
20. Welche Geschäftsbeziehungen unterhielt oder unterhält das BMI mit der Schweizer Firma N., die nach Medienberichten IMSI-Catcher (IMSI: International Mobile Subscriber Identity) unter anderem an ein „Todesschwadron aus Bangladesch“ verkauft haben soll (WOZ Die Wochenzeitung vom 4. September 2014)?
21. Inwiefern wurde inzwischen mit dem Vorhaben „Wissenserschließung aus offenen Quellen“ (WeroQ) begonnen, bzw. aus welchem Grund ist ein Zuwendungsbescheid durch das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr an das Fraunhofer-Institut immer noch nicht erfolgt (Schreiben des BMI an den Abgeordneten Andrej Hunko vom 22. Juli 2014)?
- a) Welche „Textmining-Technologien“ sollen konkret untersucht werden?
- b) Welche Schlussfolgerungen zieht die Bundesregierung aus einer Darstellung der Universität Rostock, die dem Schreiben des BMI vom 22. Juli 2014 hinsichtlich einer Kooperation mit dem Institut für grafische Wissensorganisation (Grawis) widerspricht (taz.die tageszeitung vom 15. August 2014)?
- c) Welche gemeinsamen Förderanträge der Universität Rostock mit dem Grawis sind der Bundesregierung bekannt?
22. Auf welche Art und Weise soll die „Echtzeitanalyse von Streaming-Daten“ durch den BND Informationsströme durchsuchen und dabei „Muster“ erkennen (Schreiben des BMI an den Abgeordneten Andrej Hunko vom 22. Juli 2014)?
- a) Mithilfe welcher statistischer Verfahren sollen aus diesen Mustern „Tendenzen, Trends und Auffälligkeiten erkannt werden“?
- b) Welche „Betreiber“ bieten nach Kenntnis der Bundesregierung welche „derartige[n] Daten (teilweise auch gegen Gebühr)“ zur Nutzung an?
23. Inwiefern trifft es, wie den Fragestellern bekannt ist, zu, dass das BKA eine Lizenz für die Software „IBM Content Analytics“ zur Vorhersage bzw. Erstellung von Prognosen zukünftiger Straftaten beschafft?
- a) Aus welchem Grund wurde das Projekt nicht auf Bundestagsdrucksache 18/707 (Frage 1) vom März 2014 beauskunftet?
- b) Welche Laufzeit hat ein entsprechendes Forschungsprojekt, und wie wurde es ausgeschrieben?
- c) Welche Details kann die Bundesregierung zum Zweck eines entsprechenden Forschungsprojektes mitteilen, und welche Kosten entstehen hierfür?
- d) Welche weiteren Teilnehmenden (auch im Unterauftrag) sind der Bundesregierung hierzu bekannt, und worin genau besteht deren jeweiliger Auftrag?
- e) Wo und auf welche Weise wird die Software getestet?
- f) Inwiefern wird die Software auch in konkreten Ermittlungsverfahren ausprobiert?
24. Mit welchen weiteren Herstellern sowie Landespolizeibehörden hatten Behörden des BMI hinsichtlich der Nutzung von Anwendungen zum „Predictive Policing“ Kontakt?

25. Welche aktuellen Marktsichtungen wurden hierzu mit welchem Ergebnis durchgeführt?
26. Welche „organisatorischen und personellen Herausforderungen, die sich aus den Entwicklungen auf dem Gebiet der Telekommunikation für die Sicherheitsbehörden ergeben“ wurden beim auf Bundestagsdrucksache 18/2257 beauskunfteten Treffen des „Runden Tisches zur Sicherstellung der Telekommunikationsüberwachung in der Zukunft des Bundesministeriums des Innern“ konkret besprochen?
27. Welche Maßnahmen hat das BMI daraufhin eingeleitet, bzw. welche weiteren Maßnahmen sind geplant?

Berlin, den 19. September 2014

Dr. Gregor Gysi und Fraktion

