Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Herrn
Fabian Keil
[redacted]

Per E-Mail:
[redacted]

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49(0)30 18 681-[redacted]
FAX +49(0)30 18 681-[redacted]
BEARBEITET VON RD[redacted]

E-MAIL ZI4@bmi.bund.de
INTERNET www.bmi.bund.de
DIENSTSITZ Berlin
DATUM 7. März 2014
AZ ZI4-13002/4#315

BETREFF **Informationsfreiheitsgesetz**
HIER Zugang zu Unterlagen, welche verschiedene Aussagen von Bundesinnenminister de Maiziére im Rahmen eines ARD-Interviews in der Reihe „Bericht aus Berlin“ am 19. Januar 2014 belegen
BEZUG Ihr Schreiben per E-Mail vom 23. Januar 2014
Meine Zwischennachricht vom 20. Februar 2014

Sehr geehrter Herr Keil,

mit o. g. Schreiben baten Sie um Unterlagen, welche verschiedene Aussagen von Bundesinnenminister Dr. Thomas de Maiziére im Rahmen eines ARD-Interviews in der Reihe „Bericht aus Berlin“ am 19. Januar 2014 belegen.

Dazu wird Ihnen im Einzelnen wie folgt Auskunft erteilt:

Aussage 1 „Selbst wenn die NSA überhaupt nicht mehr sich für das Internet interessiert, es gibt andere Staaten, die das tun und zwar viel schamloser.“ (0:36)

Aus dem aktuellen Verfassungsschutzbericht geht hervor, dass die Bundesrepublik Deutschland aufgrund ihrer geopolitischen Lage, ihrer Rolle in der Europäischen Union und in der NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie Ziel nachrichtendienstlicher Ausspähung ist. Hauptträger der Spionageaktivitäten gegen Deutschland sind derzeit die Russische Föderation und die Volksrepublik China, aber auch Länder des Nahen und Mittleren Ostens (vgl. Verfassungsschutzbericht 2012, S. 374 ff.).

ZUSTELL- UND LIEFERANSCHRIFT Alt Moabit 101 D, 10559 Berlin
VERKEHRSANBINDUNG S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Aussage 2 „Es gibt die organisierte Kriminalität, die sich für das Netz interessiert, die wollen an unsere Überweisungen." (0:42)

In dem im Jahr 2012 veröffentlichten Bundeslagebild Cybercrime weist das Bundeskriminalamt (BKA) auf die vielfältigen Bedrohungen durch Cybercrime hin, dessen Gefährdungs- und Schadenspotenzial unverändert hoch ist. Eine der Erscheinungsformen ist die Ausspähung aller Formen und Arten der digitalen Identitäten, darunter auch Zugangsdaten im Bereich des Onlinebanking, und deren Einsatz für kriminelle Zwecke (vgl. BKA Cybercrime - Bundeslagebild 2012).

Aussage 3 „Der Schutz des Internet, gegen wen auch immer, das ist unsere gemeinsame Aufgabe und nicht nur die Fixierung auf die NSA." (0:58)

Die neue Bundesregierung wird Daten-, Netz- und Informationssicherheit zu einem Schwerpunkt ihrer Arbeit machen und sich dafür einsetzen, die Informations- und Kommunikationssicherheit in Deutschland und Europa grundlegend zu stärken. Dies geht bereits aus dem Koalitionsvertrag für die 18. Legislaturperiode hervor (vgl. Koalitionsvertrag S. 147 ff). Gleichwohl ist dies eine gemeinsame Aufgabe von Wirtschaft, Staat und Zivilgesellschaft. Konkret angestrebt wird u.a.

- die Unterstützung von mehr und besserer Verschlüsselung bei den Nutzern,
- die Förderung vertrauenswürdiger Hersteller und Dienstleister in Deutschland, um auf deren Technologien aufbauen zu können,
- die Verabschiedung eines IT-Sicherheitsgesetzes, mit dem die Betreiber Kritischer Infrastrukturen ebenso in die Verantwortung genommen werden sollen wie die Provider,
- die Prüfung von Möglichkeiten für ein europäisches Routing bzw. eine europäische oder deutsche Cloud und
- die Ermunterung von Unternehmen, in ihren Bereichen dem Beispiel der deutschen E-Mail-Anbieter zu folgen, und ebenfalls stärker Verschlüsselung zu nutzen.

Aussage 4 „Wir dürfen allerdings auch die Zusammenarbeit der Dienste nicht per se verteufeln, wir brauchen sie zur Terror-Bekämpfung." (1:32)

Die Sicherheitsbehörden des Bundes sind zur Wahrnehmung ihrer gesetzlichen Aufgaben auf den Austausch mit internationalen Partnern wie beispielsweise mit US-amerikanischen Stellen angewiesen. In der Vergangenheit waren solche Hinweise

Grundlage für die Verhinderung schwerer Straftaten durch deutsche Behörden. Der Austausch von Daten und Hinweisen erfolgt dabei anlassbezogen im Rahmen der Aufgabenerfüllung ausschließlich nach den hierfür vorgesehenen gesetzlichen Übermittlungsbestimmungen.

Diesbezüglich wird auf die BT-Drs. 17/14560 (Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD – Drucksache 17/14456 – Abhörprogramme der ... mit den US-Nachrichtendiensten), insbesondere auf die Antworten zu den Fragen 34 ff. verwiesen.

Aussage 5 „... das SWIFT-Abkommen hilft auch der Terror-Bekämpfung ..." (2:09)

Gemäß Artikel 2 des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (sog. SWIFT-Abkommen) ist es dessen Ziel, „unter uneingeschränkter Achtung der Privatsphäre und des Schutzes personenbezogener Daten und der übrigen in diesem Abkommen festgelegten Bedingungen sicherzustellen, dass

a. Zahlungsverkehrsdaten und damit verbundene Daten, die von gemäß diesem Abkommen gemeinsam bezeichneten Anbietern von internationalen Zahlungsverkehrsdatendiensten im Gebiet der Europäischen Union gespeichert werden, dem US-Finanzministerium ausschließlich für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Terrorismus oder Terrorismusfinanzierung bereitgestellt werden und
b. sachdienliche Informationen, die im Wege des TFTP (Terrorist Finance Tracking Programm) erlangt werden, den für die Strafverfolgung, öffentliche Sicherheit oder Terrorismusbekämpfung zuständigen Behörden der Mitgliedstaaten, Europol oder Eurojust für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Terrorismus und Terrorismusfinanzierung zur Verfügung gestellt werden."

Aussage 6 „Die Safe-Harbor-Regelung hilft deutschen Unternehmen, dass sie nicht Probleme [be]kommen, wenn sie Daten übermitteln." (2:10)

Bei Safe Harbor handelt es sich um eine zwischen der EU und den USA im Jahre 2000 getroffene Vereinbarung, die die zentrale Grundlage für Datenübermittlungen der Wirtschaft an Unternehmen in den USA bildet. Safe Harbor enthält eine Reihe

von Garantien zugunsten der Bürgerinnen und Bürger. Es handelt sich um eine Art Zertifizierungsmodell, nach dem sich Unternehmen verpflichten, bestimmte Grundsätze und Prinzipien einzuhalten. Auch wenn der Beitritt zu Safe Harbor freiwillig ist, sind die Unternehmen danach verpflichtet, sich an die Grundsätze von Safe Harbor zu halten und müssen dies der Federal Trade Commission (FTC) jährlich mitteilen (vgl. Pressemitteilung des Bundesministeriums des Innern zum Treffen der Justiz- und Innenminister zum informellen Rat in Athen vom 23. Januar 2014).

Aussage 7: „Man muss nicht sein Tagebuch ins Internet stellen. Eine E-Mail ist faktisch wie eine Postkarte. Da kann man nicht erwarten, dass sie so geschützt wird, wie ein verschlossener Brief. Wir sollen nicht so viel ins Internet stellen." (2:49)

Die Aussage basiert auf der Funktionsweise des der E-Mail zugrundeliegenden technischen Verfahrens und lässt sich z.B. anhand einer Einschätzung des Bundsamtes für Sicherheit in der Informationstechnik (BSI) nachvollziehen, das sich bezüglich der Notwendigkeit von Verschlüsselungstechniken für E-Mails und Dateien wie folgt äußert:

„Beim altmodischen Briefschreiben haben wir die Inhalte unserer Mitteilungen ganz selbstverständlich mit einem Briefumschlag geschützt. Der Umschlag schützt die Nachrichten vor fremden Blicken, eine Manipulation am Umschlag kann man leicht bemerken. Nur wenn etwas nicht ganz so wichtig ist, schreibt man es auf eine ungeschützte Postkarte, die auch der Briefträger oder andere lesen können.
Ob die Nachricht wichtig, vertraulich oder geheim ist, das bestimmt man selbst und niemand sonst. Eine normale E-Mail ist immer offen wie eine Postkarte, und der elektronische „Briefträger" - und andere - können sie immer lesen. Die Sache ist sogar noch schlimmer: Die Computertechnik bietet nicht nur die Möglichkeiten, die vielen Millionen E-Mails täglich zu befördern und zu verteilen, sondern auch, sie zu kontrollieren, auszuwerten oder sogar unbemerkt zu verändern."
(https://www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html)

Aussage 8: „Es ist eine staatliche Aufgabe, Angriffe auf das Internet, von wem auch immer, besser zu schützen als bis her." (3:02)

Gemäß der Cyber-Sicherheitsstrategie für Deutschland aus dem Jahr 2011 ist es das Ziel der Bundesregierung, einen signifikanten Beitrag für einen sicheren Cyber-

Raum zu leisten. Dadurch sollen die wirtschaftliche und gesellschaftliche Prosperität für Deutschland bewahrt und gefördert werden.
Dabei ist die Cyber-Sicherheit in Deutschland auf einem der Bedeutung und der Schutzwürdigkeit der vernetzten Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. Der Zustand eines sicheren Cyber-Raums ergibt sich dabei als Summe aller nationalen und internationalen Maßnahmen zum Schutz der Verfügbarkeit der Informations- und Kommunikationstechnik sowie der Integrität, Authentizität und Vertraulichkeit der sich darin befindenden Daten.
(vgl. Cyber-Sicherheitsstrategie für Deutschland, Feb. 2011, S. 4). Im Übrigen wird auch auf die Ausführungen zu Aussage 3 verwiesen.

Diese Auskunft ergeht kostenfrei.

Ich hoffe, ich konnte Ihnen mit meinen Ausführungen weiterhelfen.

Mit freundlichen Grüßen
Im Auftrag
[redacted]