

Antrag
der Fraktionen CDU/CSU, SPD, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

Einsetzung eines Untersuchungsausschusses

Der Bundestag wolle beschließen:

A. Einsetzung

I. Es wird ein Untersuchungsausschuss eingesetzt.

II. Der Untersuchungsausschuss soll aus 8 Mitgliedern und entsprechend vielen Stellvertretern bestehen.

B. Auftrag

Der Untersuchungsausschuss soll – angestoßen insbesondere durch Presseberichterstattung in Folge der Enthüllungen von Edward Snowden über Internet- und Telekommunikationsüberwachung – für den Zeitraum seit Jahresbeginn 2001 klären,

I. ob, in welcher Weise und in welchem Umfang durch Nachrichtendienste der Staaten der sogenannten „Five Eyes“ (der Vereinigten Staaten von Amerika, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands) eine Erfassung von Daten über Kommunikationsvorgänge (einschließlich Inhalts-, Bestands- und Verkehrsdaten), deren Inhalte sowie sonstige Datenverarbeitungsvorgänge (einschließlich Internetnutzung und angelegter Adressverzeichnisse) von, nach und in Deutschland auf Vorrat oder eine Nutzung solcher durch öffentliche Unternehmen der genannten Staaten oder private Dritte erfasster Daten erfolgte beziehungsweise erfolgt und inwieweit Stellen des Bundes, insbesondere die Bundesregierung, Nachrichtendienste oder das Bundesamt für Sicherheit in der Informationstechnik von derartigen Praktiken Kenntnis hatten, daran beteiligt waren, diesen entgegenwirkten oder gegebenenfalls Nutzen daraus zogen. Hierzu soll der Ausschuss im Einzelnen prüfen:

1. Wurden durch Überwachungsprogramme des US-amerikanischen Nachrichtendienstes „National Security Agency“ (NSA) und des britischen „Government Communications Headquarters“ (GCHQ) oder durch Unternehmen in ihrem Auftrag Daten (insbesondere über Telekommunikationsvorgänge einschließlich SMS, Internet-Nutzung, E-Mail-Verkehr („C2C“), Nutzung sozialer Netzwerke und elektronischer Zahlungsverkehr) einer

Erfassung und Speicherung auf Vorrat sowie einer Kontrolle und Auswertung unterzogen, von der auch Kommunikations- und Datenverarbeitungsvorgänge von, nach und in Deutschland betroffen waren? Erfolgte Entsprechendes bei deutschen Staatsangehörigen, die sich im Hoheitsbereich eines der unter Nummer I. genannten Länder oder in einem Mitgliedsland der EU aufhielten? Erfolgte Entsprechendes durch andere Dienste der unter I. genannten Länder? Seit wann, wie, in welchem Umfang und gegebenenfalls auf welchen Rechtsgrundlagen erfolgte dies?

2. Inwieweit wurden und werden dabei diplomatische Vertretungen und militärische Standorte genutzt, um Daten über solche Kommunikations- und Datenverarbeitungsvorgänge und deren Inhalte zu gewinnen?

3. Gegen welche Rechtsvorschriften auf deutscher, europäischer und internationaler Ebene verstießen oder verstoßen derartige Aktivitäten gegebenenfalls?

4. Haben und gegebenenfalls seit wann haben die Bundesregierung, ihr nachgeordnete Dienststellen oder durch sie mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte Hinweise darauf oder positive Kenntnis von in den Nummern I. oder 1. genannten Vorgängen? Haben sie eine Beteiligung von Stellen des Bundes oder von ihnen mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragter hieran gekannt, gebilligt, unterstützt oder angeordnet?

5. Haben und gegebenenfalls seit wann haben die Bundesregierung, ihr nachgeordnete Dienststellen oder durch sie mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte Hinweise auf oder positive Kenntnis von in den Nummern I. oder 1. genannten Aktivitäten zu Lasten von anderen Mitgliedstaaten der EU oder der NATO, deren Bevölkerung oder dort ansässigen Unternehmen? Wie wurden solche Kenntnisse gegebenenfalls bewertet und welche Schlüsse daraus gezogen?

6. Welche Vorkehrungen oder Maßnahmen haben Stellen des Bundes ergriffen oder veranlasst beziehungsweise hätten sie ergreifen oder veranlassen müssen, um die in den Nummern I. oder 1. genannten Aktivitäten und ihr Ausmaß gegebenenfalls festzustellen und zu unterbinden? Inwieweit, bis wann und weshalb unterblieb dies gegebenenfalls und wer trägt dafür die Verantwortung?

7. Haben Stellen des Bundes oder durch sie mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte Daten aus den in den Nummern I. oder 1. genannten Aktivitäten erlangt oder genutzt sowie dafür möglicherweise Gegenleistungen erbracht? Waren Stellen des Bundes oder von ihnen mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte Teil eines systematisierten wechselseitigen oder „Ring“-Tausches geheimdienstlicher Informationen, in dem der jeweils anderen Seite Daten oder Erkenntnisse übermittelt werden, die diese nach dem jeweils am Ort der Datenerhebung geltenden Recht selbst nicht erheben darf? Auf welcher Rechtsgrundlage und zu welchem Zweck wurden oder werden derartige Daten gegebenenfalls erlangt oder genutzt? Wie wurde gegebenenfalls sichergestellt, dass die betreffenden Informationen auch nach deutschem Recht erlangt und genutzt werden dürfen? Wie wurde gegebenenfalls sichergestellt, dass nicht Informationen erlangt und genutzt wurden und werden, die nach deutschem Recht nicht hätten erhoben werden dürfen?

8. Waren Stellen des Bundes oder von ihnen mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte an der Entwicklung beziehungsweise technischen Umsetzung oder Anwendung von Programmen wie „PRISM“, „TEMPORA“, „XKeyscore“ oder anderer, von Diensten der in Nummer I. genannten Länder oder in deren Auftrag für die in den Num-

mern I. oder 1. genannten Aktivitäten genutzter Programme in irgendeiner Form beteiligt? Wer auf deutscher Seite war gegebenenfalls wie, wie lange und woran im Einzelnen beteiligt?

9. Haben Stellen des Bundes oder von ihnen mit sicherheitsrelevanten (auch IT-) Aufgaben Beauftragte von der NSA, dem GCHQ oder anderen Diensten der in Nummer I. genannten Länder selbst oder in deren Auftrag entwickelte Programme erhalten, erprobt oder genutzt und haben sie dabei auch auf Datenbestände zugegriffen, die aus in den Nummern I. oder 1 genannten Kommunikations- und Datenverarbeitungsvorgängen stammten? Wer auf deutscher Seite hat gegebenenfalls welche Programme erhalten, diese wie lange erprobt oder genutzt und dabei auf welche der genannten Datenbestände zugegriffen?

10. Welche Erkenntnisse über Art und Ausmaß derartiger Aktivitäten, die sich gegen in der Bundesrepublik Deutschland ansässige Wirtschaftsunternehmen richten, lagen Stellen des Bundes wann vor?

11. Hätten Stellen des Bundes gegebenenfalls schon zu einem früheren Zeitpunkt von derartigen Maßnahmen Kenntnis erlangen können beziehungsweise müssen? Gegebenenfalls welche Stellen wann?

12. Inwieweit wurde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unverzüglich über Erkenntnisse und Informationen unterrichtet, die geeignet waren, den Verdacht auf Verletzung datenschutzrechtlicher Bestimmungen zu begründen? Weshalb und aufgrund welcher Umstände und Einflussnahmen unterblieb dies gegebenenfalls?

13. In Anwendung welcher IT-Sicherheitskonzepte hat die Bundesregierung in ihrem Verantwortungsbereich Gestaltung und Betrieb von Telekommunikations- und IT-Strukturen, Dateien, Registern und Verwaltungsprozessen gegen unberechtigten Datenabfluss und -Zugriff Dritter gesichert?

14. Haben US-amerikanische Stellen auf deutschem Staatsgebiet oder von diesem ausgehend Telekommunikationsüberwachungen, Festnahmen oder gezielte Tötungen durch Kampfdrohneinsätze durchgeführt oder veranlasst? Welche Erkenntnisse lagen Stellen des Bundes zu welchem Zeitpunkt hierüber gegebenenfalls vor? Waren sie an der Vorbereitung oder Durchführung derartiger Maßnahmen gegebenenfalls in irgendeiner Form beteiligt oder haben sie gebilligt? Welche Reaktionen auf solche Erkenntnisse waren gegebenenfalls geboten und welche wurden ergriffen?

15. Inwiefern haben die Bundesregierung sowie die ihr nachgeordneten Dienststellen US-amerikanischen Sicherheitsbehörden ermöglicht, an Befragungen von Asylbewerbern teilzunehmen oder solche Befragungen eigenständig durchzuführen?

16. Welche Tätigkeiten haben die Bundesregierung nebst ihr nachgeordnete Dienststellen gegebenenfalls je wann ergriffen, um auf eine Aufklärung, Strafverfolgung und Beendigung dieser Praktiken hinzuwirken, beziehungsweise weshalb und gegebenenfalls aufgrund welcher Umstände und Einflussnahmen ist dies unterblieben?

17. Waren die von der Bundesregierung der Öffentlichkeit mitgeteilten Informationen zu den vorgenannten Fragen zutreffend? Waren die von der Bundesregierung gegenüber Abgeordneten oder parlamentarischen Institutionen mitgeteilten Informationen zu den vorgenannten Fragen zutreffend und umfassend? Hat die Bundesregierung alle bestehen-

den gesetzlichen Informationspflichten gegenüber dem Parlamentarischen Kontrollgremium, der G10-Kommission sowie dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erfüllt? Sind diesen Kontrollinstitutionen relevante Informationen vorenthalten worden?

II. ob und inwieweit Daten über Kommunikationsvorgänge und deren Inhalte (mittels Telekommunikation oder Gesprächen einschließlich deren Inhalte wie etwa Gesetzentwürfe oder Verhandlungsstrategien) von Mitgliedern der Bundesregierung, Bediensteten des Bundes sowie Mitgliedern des Deutschen Bundestages oder anderer Verfassungsorgane der Bundesrepublik Deutschland, durch Nachrichtendienste der unter I. genannten Staaten nachrichtendienstlich erfasst oder ausgewertet wurden. Hierzu soll der Ausschuss prüfen:

1. Wurde der Datenverkehr von Stellen des Bundes durch Nachrichtendienste der genannten Staaten erfasst oder überwacht? Waren hiervon auch deutsche Vertretungen im Ausland betroffen? Gegebenenfalls seit wann, wie und in welchem Umfang?

2. Wurde Telekommunikation (Telefongespräche, SMS, E-Mails etc.) oder Internetnutzung von Mitgliedern der Bundesregierung und Bediensteten des Bundes sowie von Mitgliedern des Deutschen Bundestages oder anderer Verfassungsorgane der Bundesrepublik Deutschland durch Nachrichtendienste der genannten Staaten erfasst oder ausgewertet? Seit wann und in welchem Umfang erfolgte dies?

3. Weshalb wurden gegebenenfalls derartige Kommunikationserfassungen von Stellen des Bundes nicht früher bemerkt und unterbunden?

4. Welche Strategie zum Schutz vor unberechtigtem Zugriff auf Daten oder Abfluss von Daten aus IT-Systemen des Bundes hat die Bundesregierung im Untersuchungszeitraum verfolgt und wie wurde diese weiterentwickelt?

5. Waren die von der Bundesregierung der Öffentlichkeit mitgeteilten Informationen zu den vorgenannten Fragen zutreffend? Waren die von der Bundesregierung gegenüber Abgeordneten oder parlamentarischen Institutionen mitgeteilten Informationen zu den vorgenannten Fragen zutreffend und umfassend? Hat die Bundesregierung alle bestehenden gesetzlichen Informationspflichten gegenüber dem Parlamentarischen Kontrollgremium, der G10-Kommission sowie dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erfüllt? Sind diesen Kontrollinstitutionen relevante Informationen vorenthalten worden?

III. ob Empfehlungen zur Wahrung des verfassungsrechtlich gewährleisteten Schutzes der informationellen Selbstbestimmung, der Privatsphäre, des Fernmeldegeheimnisses und der Integrität und Vertraulichkeit informationstechnischer Systeme sowie der sicheren und vertraulichen Kommunikation in der staatlichen Sphäre geboten sind. Hierzu soll der Ausschuss klären:

1. Sind rechtliche und technische Veränderungen am deutschen System der nachrichtendienstlichen Auslandsüberwachung nötig, um der Grund- und Menschenrechtsbindung deutscher Stellen vollauf gerecht zu werden und gegebenenfalls welche?

2. Sind rechtliche und technische Veränderungen bezüglich der Übermittlung, Entgegennahme und des Austausches von Informationen mit ausländischen Sicherheitsbehörden

nötig, um der Bindung der Bundesregierung und aller deutschen Stellen an die Grund- und Menschenrechte vollauf gerecht zu werden und gegebenenfalls welche?

3. Durch welche Maßnahmen rechtlicher, organisatorischer oder technischer Art kann sichergestellt werden, dass der garantierte Schutz der Vertraulichkeit der elektronischen Kommunikation von, nach und in Deutschland bestmöglich verwirklicht wird, damit Bürgerinnen und Bürger sowie Träger von Berufsgeheimnissen und Zeugnisverweigerungsrechten und Träger von Betriebs- und Geschäftsgeheimnissen vor einer verdachtsunabhängigen Erfassung von elektronischen Kommunikationsvorgängen und deren Inhalten durch ausländische Nachrichtendienste geschützt werden?

4. Welche Maßnahmen sind erforderlich, um eine vertrauliche elektronische Kommunikation auch für staatliche Stellen zu gewährleisten?

5. Sind zum Schutze der Telekommunikations- und IT-Sicherheit künftig Veränderungen bei der Vergabe öffentlicher Aufträge nötig ?

6. Welche Maßnahmen zur Gewährleistung eines bestmöglichen Schutzes der Privatheit der elektronischen Kommunikation sind auf europäischer und internationaler Ebene erforderlich? Hierzu sollen die Erkenntnisse der Untersuchung im LIBE-Ausschuss des Europäischen Parlaments sowie die Arbeiten auf Ebene der Vereinten Nationen einbezogen werden.

7. Welche Maßnahmen sind nötig, um die Bevölkerung, Unternehmen und öffentliche Verwaltung besser vor Internet- und Telekommunikationsüberwachung durch ausländische Stellen zu schützen?

8. Wie kann die exekutive, parlamentarische, justizielle und unabhängige datenschützerische Kontrolle der Sicherheitsbehörden des Bundes lückenlos und effektiv gewährleistet werden?

9. Welche sonstigen rechtlichen, technisch-infrastrukturellen und politischen Konsequenzen sind zu ziehen?

Berlin, den

Volker Kauder, Gerda Hasselfeldt und Fraktion
Thomas Oppermann und Fraktion
Dr. Gregor Gysi und Fraktion
Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion