

## **Antwort**

### **der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.  
– Drucksache 18/11331 –**

### **Geheimdienstbericht zu russischen Aktivitäten im Cyberraum**

#### Vorbemerkung der Fragesteller

Ein vom Bundeskanzleramt beauftragter Geheimdienstbericht zu russischen Aktivitäten im Cyberraum bleibt unter Verschluss (Bundestagsdrucksache 18/11106, Frage 7). Die Überprüfung dort gesammelter Behauptungen ist Abgeordneten also unmöglich. Einen Tag, bevor die Abgeordneten von der Geheimhaltung erfahren, wird das Papier einem Journalisten zugespielt (tageschau.de vom 6. Februar 2017, „Keine ‚Smoking Gun‘ aus Russland“). Laut dessen Bericht hätten die Geheimdienste keine Beweise für eine russische Desinformationskampagne gefunden. Trotzdem habe das Bundeskanzleramt weitere Untersuchungen angewiesen.

Das Narrativ, wonach vor allem der Kreml für digitale Bedrohungen verantwortlich sein soll, wird von den Fragestellern angezweifelt. Einmal pro Woche melde das Bundesamt für die Sicherheit in der Informationstechnik laut dem Bundesministerium des Innern einen „Angriff mit mutmaßlich nachrichtendienstlichem Hintergrund“. Der Verfassungsschutz hat dies aber in keinem der Fälle bestätigen können. Viele der Angriffe werden aus Sicht der Fragesteller verzerrt dargestellt. So definiert die Staatssekretärin im Bundesministerium des Innern Dr. Emily Haber auf Bundestagsdrucksache 18/11106 einen Vorfall als „hochspezialisierten Cyberangriff“, wenn dieser einen Virenschanner umgehen kann. Der im Dezember 2016 verlautbarte „groß angelegte Hackerangriff“ auf die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) entpuppt sich in der Antwort auf die Kleine Anfrage als Phishing-Mail, die nach Anklicken eines gefälschten Links einen lange bekannten Trojaner nachlud. Die behauptete russische Urheberschaft kann auch hier nicht belegt werden.

#### Vorbemerkung der Bundesregierung

1. Die Beantwortung der Fragen 11, 15b und 17 sowie in Teilen der Frage 15a kann aus Gründen des Staatswohls nicht in offener Form erfolgen. Aus ihrem Bekanntwerden können Rückschlüsse auf die Arbeitsweise und Methode der Nachrichtendienste des Bundes gezogen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts besonders schutzbedürftig sind (BVerfGE 124,

161 (194)). Hierdurch würde die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt, was wiederum die Sicherheit der Bundesrepublik Deutschland gefährdet. Diese Informationen werden daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

2. Die Bundesregierung ist nach sorgfältiger Abwägung ferner zu der Auffassung gelangt, dass eine Beantwortung der Frage 2 aus Gründen des Staatswohls nicht offen erfolgen kann. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung ihres gesetzlichen Auftrags besonders schutzwürdig. Ebenso schutzbedürftig sind Einzelheiten zur nachrichtendienstlichen Erkenntnislage. Eine Veröffentlichung von Einzelheiten solche Erkenntnisse betreffend würde zu einer wesentlichen Schwächung der zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftrags Erfüllung erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS-Vertraulich“ eingestuft und werden in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

3. Die Frage 4 sowie in Teilen Frage 8 berühren solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufte Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten bekannt würden, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Zusammenarbeit mit ausländischen Partnern besonders schutzbedürftig sind.

Eine öffentliche Bekanntgabe von Informationen zum Kenntnisstand, zur Leistungsfähigkeit, zur Ausrichtung und zu technischen Fähigkeiten von ausländischen Partnerdiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland.

Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich auch der gesetzliche Auftrag des Bundesnachrichtendienstes – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst [BNDG]) - nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung von auslandsbezogenen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des Bundesnachrichtendienstes jedoch unerlässlich.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung der Nachrichtendienste

des Bundes nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben ihre Fähigkeiten und Arbeitsweisen so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

1. Aus welchen Gründen hat die Bundesregierung entschieden, den Geheimdienstbericht zu vermeintlich russischen Aktivitäten im Cyberraum „nur für den internen Gebrauch“ einzustufen und auch Abgeordneten nicht zugänglich zu machen?

Der Bericht beinhaltet Informationen aus nachrichtendienstlichem Aufkommen, welche gemäß VSA als Verschlussache eingestuft sind. Es handelt sich um einen laufenden Vorgang der Bundesregierung. Im Übrigen ergibt sich aus dem parlamentarischen Fragerecht lediglich ein Anspruch gegen die Bundesregierung auf Beantwortung gestellter Fragen, aber kein Recht auf die Zugänglichmachung von Dokumenten.

2. Welche einzelnen Fragestellungen wurden von den Geheimdiensten untersucht?

Die Antwort auf diese Frage ist als Verschlussache mit dem VS-Grad „VS-Vertraulich“ eingestuft und wird in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.\*

3. Inwiefern wurde die zur Erstellung des nunmehr vorliegenden Geheimdienstberichtes eingerichtete „temporäre Arbeitseinheit“ wie angekündigt aufgelöst (Bundestagsdrucksache 18/10759, Antwort zu Frage 7)?

Die im Bundesamt für Verfassungsschutz (BfV) gebildete temporäre Arbeitseinheit wurde nicht aufgelöst.

4. Welche Abteilungen gehörten dieser „temporären Arbeitseinheit“ an?

Nähere Angaben können aus Gründen des Staatswohls nicht erfolgen, da dies die Arbeitsweise des BfV offenlegen und damit die Grundlage seiner Aufgabenerfüllung beeinträchtigen würde. Auf die Vorbemerkung der Bundesregierung wird verwiesen.

---

\* Das Bundesministerium des Innern hat die Antwort als „VS – Vertraulich“ eingestuft.

Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

5. Was ist der Bundesregierung darüber bekannt, welche Regierungsmitarbeiter den nicht öffentlichen Geheimdienstbericht an einen Journalisten weitergaben (tagesschau.de vom 6. Februar 2017, „Keine ‚Smoking Gun‘ aus Russland“)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

6. Inwiefern und aus welchen Gründen trifft es zu, dass das Bundeskanzleramt trotz des ergebnislosen Geheimdienstberichtes weitere Untersuchungen zu einer russischen Desinformationskampagne oder ähnlichen Phänomenen anordnete?

Über die im Lagebericht zusammengestellten Erkenntnisse hinaus beobachtet die Bundesregierung aufmerksam und fortlaufend die verstärkten russischen Aktivitäten in Deutschland, aber auch in anderen europäischen Staaten.

7. Welche Behörden sind hiermit befasst, und inwiefern bilden diese abermals eine „temporäre Arbeitseinheit“?

Die Sicherheitsbehörden des Bundes sind weiterhin im Rahmen ihres gesetzlichen Auftrags mit diesem Thema befasst und tauschen sich dazu regelmäßig aus.

8. Welche weiteren Details kann die Bundesregierung zu der von „tagesschau.de“ berichteten künftigen „Zusammenarbeit“ deutscher Geheimdienste mit Frankreich und den Niederlanden mitteilen?

Die Nachrichtendienste des Bundes tauschen sich auf der Basis der gesetzlichen Regelungen regelmäßig mit Partnerdiensten der Mitgliedstaaten der Europäischen Union oder der NATO aus. Dieser Austausch erfolgt auf der Grundlage gegenseitiger Vertraulichkeit. Nähere Angaben können aus Gründen des Staatswohls nicht erfolgen, da dies die Grundlage der Zusammenarbeit gefährden würde. Dies wiederum würde sich nachteilig auf die Interessen der Bundesrepublik Deutschland auswirken.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

9. Welche Arbeitsaufträge ergingen dazu an welche Behörden beider Seiten?

Auf die Antwort zu Frage 8 wird verwiesen.

10. Welche technischen Vorkehrungen gegen erwartete „vielfältige Angriffsstrategien durch Cyberattacken“, „Falschmeldungen“ sowie zur Absicherung der Ergebnisübermittlung trifft der Bundeswahlleiter angesichts einer befürchteten Beeinflussung der Bundestagswahl im Herbst 2017 durch die russische Regierung (tagesspiegel.de vom 15. Januar 2017, „Wahlleiter stellt sich auf Hackerangriffe und Fake News ein“)?

#### Cyberangriffe

Die IT-Infrastruktur des Bundeswahlleiters wird stets unter der Prämisse einer sicheren Durchführung der Wahlen konzipiert bzw. fortentwickelt. Dies schließt eine hochverfügbare Infrastruktur zur Ermittlung des Wahlergebnisses ebenso ein wie den Schutz der Integrität der Wahlergebnisse und die Vertraulichkeit der relevanten Daten. Der Bundeswahlleiter stützt sich dabei auf die etablierten IT-Sicherheits- und -Managementinfrastrukturen des Statistischen Bundesamtes und des IT-Dienstleisters des Bundes ITZBund.

Die hohen Sicherheitsanforderungen im Rahmen der IT-Unterstützung der Wahlen sind sowohl in der Gesamtarchitektur der informationstechnischen Realisierung als auch in speziellen Sicherheitsmaßnahmen berücksichtigt. Ein wesentlicher Faktor zur Sicherstellung eines reibungslosen Ablaufs der Bundestagswahl ist die enge und vertrauensvolle Zusammenarbeit mit dem ITZBund, das für die betriebliche Realisierung verantwortlich ist.

Die spezifisch für die Wahlabwicklung durchgeführten Sicherheitsanalysen, die daraus abgeleiteten umfassenden Maßnahmenpakete sowie sehr umfangreiche Funktions-, Sicherheits- und Ausfalltests und Notfallvorsorgemaßnahmen haben bei den letzten Wahlen überzeugt. Auf dieser Basis und unter Einbeziehung der inzwischen fortentwickelten Sicherheitsmaßnahmen erfolgt derzeit eine Aktualisierung der Sicherheitskonzeption und der Dokumentation im Hinblick auf neue Erfordernisse der Bundestagswahl 2017.

Zur weiteren Bewertung der Sicherheitskonzeption und der ergriffenen bzw. weiter geplanten Maßnahmen kooperiert der Bundeswahlleiter mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem ITZBund, um auf neue Erkenntnisse reagieren zu können und in ausreichendem Maße Gegenstrategien sicherzustellen.

#### Falschmeldungen

Der Umgang mit Falschmeldungen im Zusammenhang mit wahlvorbereitendem Wahlkampf obliegt in erster Linie dem politischen Raum. Um hingegen Falschmeldungen, die der Aufgabenstellung des Bundeswahlleiters zugeordnet werden könnten, rechtzeitig zu erkennen und deren Auswirkung zu begegnen, werden unterschiedliche Maßnahmen erarbeitet. Insbesondere werden Meldungen in Medien und vor allem soziale Netzwerke beobachtet, um erforderlichenfalls umgehend entsprechend reagieren zu können.

11. Wie viele der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durchschnittlich ein Mal pro Woche an das Bundesamt für Verfassungsschutz gemeldeten „elektronischen Angriffe“ wurden von dem Geheimdienst nach einer Überprüfung tatsächlich Regierungen zugeordnet?

Die Antwort auf diese Frage ist als Verschlussache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.\*

12. Welche „universitäre Infrastruktur“ wurde im Jahr 2016 mutmaßlich durch die Kampagne APT28 kompromittiert und als Command and Control-Server „zweckentfremdet“?
13. Welche Behörden der Bundesregierung oder der Länder sind hierzu mit Ermittlungen oder einem Prüfvorgang befasst?
14. Welche Angriffe wurden über den Server vorgenommen?

Die Fragen 12 bis 14 werden gemeinsam beantwortet. Zu einer durch die Kampagne APT28 kompromittierten und als Command and Control-Server „zweckentfremdeten universitären Infrastruktur“ liegen der Bundesregierung

---

\* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

keine Erkenntnisse vor. Es sind insofern keine Behörden mit Ermittlungen oder einem Prüfungsvorgang befasst.

15. Was ist der Bundesregierung über die Funktionsweise des im Jahr 2013 entdeckten Trojaners „MiniDuke“ bekannt, der nach Medienberichten eine Lücke im Adobe Reader ausnutzte und nach einer Infektion über Google und Twitter Verbindungen mit Kontrollservern aufnehmen und weitere Malware nachladen soll (heise.de vom 27. Februar 2013, „MiniDuke: Hochspezialisierte Malware zielt auf Entscheider“)?

Der Bundesregierung liegen keine darüber hinausgehenden Erkenntnisse vor.

- a) Bei welchen Cyberangriffen auf Infrastrukturen des Bundes wurde „MiniDuke“ oder dessen Derivate von den ermittelnden Behörden entdeckt?

APT 29 wurde im Februar 2014 im Zusammenhang mit einem Angriff auf eine Bundestagsabgeordnete beobachtet. Die restliche Teil-Antwort ist als Verschluss-sache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.\*

- b) Welche amerikanischen Forschungseinrichtungen oder mittel- und osteuropäische Staaten sind nach Kenntnis der Bundesregierung bereits mit „MiniDuke“ angegriffen worden (FAZ vom 25. Dezember 2016, „Häck auf Beck“)?

Die Antwort auf diese Frage ist als Verschluss-sache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.\*

- c) Seit wann wird „MiniDuke“ vom BSI nicht mehr nur als „isolierter Komplex“ betrachtet, sondern „aufgrund von technischen Merkmalen dem größeren Komplex APT 29“ zugeordnet?

Die Bezeichnungen CozyBear und APT29 für MiniDuke werden im BSI seit etwa Februar 2015 verwendet.

- d) Welche Analysen der Firma Trend Micro sind der Bundesregierung zu „MiniDuke“ bekannt?

Der Bundesregierung sind keine Analysen der Firma TrendMicro zu „MiniDuke“ bekannt.

16. Wann erhielt das Bundeskanzleramt offiziell Kenntnis davon, dass der nationale Sicherheitsberater des US-Präsidenten, Michael Flynn, über enge Kontakte zum russischen Geheimdienst in Washington verfügte (Guardian vom 15. Februar 2017, „Damning reports emerge of Trump campaign’s frequent talks with Russian intelligence“)?

Zum Zeitpunkt der Medienberichterstattung über die genannten Vorwürfe war das Bundeskanzleramt nicht offiziell informiert.

---

\* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

17. Welche Erkenntnisse konnte der Bundesnachrichtendienst hierzu bereits im Vorfeld sammeln?

Die Antwort auf diese Frage ist als Verschlussache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.\*

18. Welche Berichte hat die deutsche Kontaktstelle der geheimdienstlichen „EU Hybrid Fusion Cell“ im Auswärtigen Amt seit deren Bestehen empfangen und verteilt?

Bislang wurden keine Berichte der EU Hybrid Fusion Cell von der Kontaktstelle im Auswärtigen Amt empfangen.

19. Was ist der Bundesregierung über die Teilnehmenden von Gesprächen der EU-Außenbeauftragten Federica Mogherini und des EU-Migrations- und Innenkommissars Dimitris Avramopoulos vom 9. und 10. Februar 2017 in den USA bekannt?
20. Welche Themen wurden dort besprochen, und inwiefern standen auch „hybride Bedrohungen“ auf der Tagesordnung?
21. Welche Ergebnisse der Gespräche sind der Bundesregierung bekannt?

Die Fragen 19 bis 21 werden gemeinsam beantwortet.

Der Bundesregierung liegen zu Gesprächen der Hohen Vertreterin der Europäischen Union (EU) für die Außen- und Sicherheitspolitik und des EU-Kommissars für Migration, Inneres und Bürgerschaft am 9. und 10. Februar 2017 in den USA keine Informationen vor.

22. Mit welchen Aufgaben ist das „Netzwerk gegen hybride Bedrohungen“ der Bundesregierung befasst?
- a) Welche einzelnen Arbeiten werden dabei von den Bundesministerien, dem Bundeskanzleramt, der Beauftragten der Bundesregierung für Kultur und Medien sowie dem Bundespresseamt übernommen?
- b) Inwiefern wurden im „Netzwerk gegen hybride Bedrohungen“ auch Leitungs- oder Sekretariatsaufgaben vergeben, und von wem werden diese übernommen?
- c) Wie oft ist das „Netzwerk gegen hybride Bedrohungen“ bereits zusammengekommen, und welche Themen standen dabei auf der Tagesordnung?

Die Fragen 22 sowie 22a bis 22c werden gemeinsam beantwortet.

Innerhalb des Netzwerks gegen hybride Bedrohungen wurde bislang keine Aufgabenverteilung vorgenommen. Auch Leitungs- oder Sekretariatsaufgaben wurden nicht vergeben. Das Netzwerk ist bislang zweimal zusammengekommen. Auf der Tagesordnung standen die Koordinierung der Netzwerkaufgaben und -aktivitäten sowie das in Gründung befindliche Hybrid-Kompetenzzentrum in Helsinki.

---

\* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

