Deutscher Bundestag **Drucksache 18/10952**

18. Wahlperiode 18.01.2017

Kleine Anfrage

der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, Sevim Dağdelen, Annette Groth, Ulla Jelpke, Katrin Kunert, Dr. Alexander S. Neu, Dr. Petra Sitte, Kersten Steinke, Kathrin Vogler und der Fraktion DIE LINKE.

Ermittlungen zu angeblich russischen Cyberangriffen

Das Bundesamt für Verfassungsschutz (BfV) verfügt laut seinem Präsidenten Dr. Hans-Georg Maaßen über „Indizien“, dass die russische Regierung im Dezember 2016 einen „Hackerangriff“ auf Computer der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) verübt habe (ZEIT ONLINE vom 7. Januar 2017, „Russland womöglich für Cyberattacke auf OSZE verantwortlich“). Der Vorfall sei demnach vom BfV selbst aufgedeckt worden. Eine Analyse habe ergeben, dass die „Angriffsinfrastruktur“ die gleiche sei, die das BfV „von anderen Cyberattacken“ kenne. Gemeint ist die mutmaßliche Gruppe „Advanced Persistent Threat“ (APT28), die im Jahr 2015 Phishing-Mails an Abgeordnete des Deutschen Bundestages versendet haben soll. Laut der Bundesregierung gebe es hierfür eine „Vielzahl von Indizien“ (Bundestagsdrucksache 18/10759).

Berichten einiger deutscher Medien zufolge seien solche „Cyberangriffe“ auch im Vorfeld der Bundestagswahl 2017 zu erwarten (beispielhaft: FAZ vom 10. November 2016, „Sicherheitskreise: Moskau kann Bundestagswahl beeinflussen“). Belege oder Quellen für ihre Behauptungen nennen die Zeitungen nicht. Entsprechende Gerüchte für eine russische Einflussnahme hatten im April 2016 bereits Dr. Hans-Georg Maaßen und der damalige Chef des Bundesnachrichtendiensts (BND), Gerhard Schindler, im Magazin „FOCUS“ gestreut (FOCUS vom 16. April 2016, „Nach diesem Interview werden Sie nicht ruhiger schlafen“). Die Geheimdienstchefs warnen darin vor „psychologische[n] Operationen“ des Kreml, darunter „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“. Auf mehrmalige Nachfrage erklärt die Bundesregierung jedoch, ihr lägen hierzu keine Erkenntnisse vor (Bundestagsdrucksachen 18/8631, 18/10313, 18/10759).

Zu den vermeintlich russischen Aktivitäten im Cyberraum hat der für die Nachrichtendienste des Bundes zuständige Staatssekretär Klaus-Dieter Fritsche einen Bericht beim BND und beim BfV beauftragt, der zwar fertiggestellt, der Öffentlichkeit oder Abgeordneten aber nicht zugänglich ist. Dadurch ist keine unabhängige Prüfung der dort zusammengetragenen Annahmen, Indizien oder Beweise möglich. Die Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion DIE LINKE. zeigen, dass die bislang vorgetragenen Vorwürfe zu angeblichen Cyberangriffen der russischen Regierung einer Überprüfung nicht standhalten: Weder sind laut der Bundesregierung Planungen zur Störung der Bundestagswahl erkennbar, noch lassen sich Medienberichte über eine angebliche Beeinflussung des Brexit-Votums untermauern. Als einzigen Beleg führt das Bundesministerium des Innern US-Untersuchungen an, die einen „Datendiebstahl“ vom Sommer 2016 auf Server der Demokraten in den USA nachweisen sollen, bei

denen E-Mails des Parteivorstands sowie des Stabs von Hillary Clinton kopiert und an die Enthüllungsplattform Wikileaks weitergereicht wurden. Ein damals betroffener Mailaccount war lediglich mit dem Passwort „password“ gesichert (http://gleft.de/1yJ).

Eine russische Urheberschaft für den Phishing-Angriff ist auch in den USA umstritten. So ist es beispielsweise kein Indiz für einen Cyberangriff aus Russland, wenn beim Programmieren eine kyrillische Tastatur verwendet wurde. Ehemalige US-Geheimdienstler bestätigen diese Auffassung (http://gleft.de/1yH). Trotzdem behaupten die US-Geheimdienste NSA, FBI und CIA weiterhin, der Phishing-Angriff auf die Demokratische Partei sei Teil einer Kampagne, die der russische Präsident Wladimir Putin persönlich angeordnet habe. Ein Anfang Januar 2017 veröffentlichter Bericht enthält in seiner deklassifizierten Version (http://gleft.de/1yL) jedoch ebenfalls keine Beweise für eine „Kampagne“ aus Russland, zu der verdeckte Geheimdienstoperationen, offene Bemühungen russischer Regierungsstellen und Staatsmedien, Eingriffe von Außenstehenden sowie bezahlte Teilnehmer sozialer Netzwerke gehören sollen.

Der Geheimdienstbericht wurde dem amtierenden (Barack Obama) sowie dem designierten (Donald Trump) Präsidenten durch den nationalen Geheimdienstdirektor James R. Clapper präsentiert, der bereits zu den Edward-Snowden-Enthüllungen der Lüge überführt wurde (http://gleft.de/1yK). Als Motivation für die angebliche russische Cyber-Kampagne nennt Clapper die Ablehnung der damaligen Präsidentschaftskandidatin Hillary Clinton. So habe der Kreml eine „deutliche Präferenz“ für den Republikaner Donald Trump entwickelt. Putin erwarte sich demnach ähnlich gute Erfahrungen von Trump, wie er sie mit dem deutschen Ex-Bundeskanzler Gerhard Schröder (SPD) gemacht habe.

Wir fragen die Bundesregierung:

1. Worin bestehen die „Indizien“, die das BfV zur Annahme verleiten, dass die russische Regierung im Dezember 2016 einen „Hackerangriff“ auf Computer der OSZE verübt haben soll (ZEIT ONLINE vom 7. Januar 2017, „Russland womöglich für Cyberattacke auf OSZE verantwortlich“)?

   a) Wann und auf welche Weise hat das BfV den Vorfall wie berichtet selbst aufgedeckt?

   b) Wie gingen die Urheber des „Hackerangriffs“ vor, und welche Werkzeuge benutzten sie dabei?

   c) Welche Schäden oder Datenabflüsse sind entstanden (bitte auch die abgeflossene Datenmenge benennen)?

   d) Von wem wurde der „Hackerangriff“ untersucht (bitte auch etwaige externe Experten benennen)?

   e) Im Rahmen welcher Untersuchungen bzw. Vorfälle im Cyberraum haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das BfV die bei der OSZE gefundene „Angriffsinfrastruktur“ bereits in der Vergangenheit beobachtet?

2. Inwiefern liegen den Geheimdiensten des Bundes seit Beantwortung der Kleinen Anfragen der Fraktion DIE LINKE. auf Bundestagsdrucksachen 18/8631, 18/10759 weiterhin „keine Erkenntnisse“ zu tatsächlich geplanten oder durchgeführten „psychologische[n] Operationen“ des Kreml vor, die laut den Präsidenten von BND und BfV „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“ beinhalten könnten?

3. Wer nahm die „Analysen der mutmaßlich russischen Cyberangriffs-Kampagnen mit internationaler Zielauswahl“ vor, aufgrund derer die Bundesregierung die „Annahme“ gründet, dass russische Geheimdienste „versuchen könnten, die Bundestagswahl 2017 durch Cyber-Angriffe zu beeinflussen“ (Bundestagsdrucksache 18/10759)?
4. Inwiefern sind aus Sicht der Bundesregierung mittlerweile konkrete Planungen zur Störung der Bundestagswahl durch die russische Regierung erkennbar?
5. Welche Behörden der Bundesregierung sind an den Ermittlungen zur Veröffentlichung vertraulicher Akten aus dem NSA-Untersuchungsausschuss durch die Enthüllungsplattform Wikileaks beteiligt, wozu die Version kursierte, Russland habe sich die Daten durch einen Cyberangriff beschafft (tagesschau.de vom 18. Dezember 2016, „Bundespolizei vermutet Maulwurf im Bundestag“)?
6. Welche Einrichtungen (Ressorts deutscher Bundesministerien sowie sonstige Teilnehmende) sind an dem im August 2016 gegründeten „Netzwerk zur Abwehr sogenannter hybrider Bedrohungen“ beteiligt, und welche Arbeitsgruppen wurden dort eingerichtet?
7. Welche Ergebnisse zeitigte die Prüfung der Ergebnisse eines Berichts, den die Bundesregierung beim BND und beim BfV zu vermeintlich russischen Aktivitäten im Cyberraum beauftragt hat (Bundestagsdrucksache 18/10759)?
   a) Sofern die Prüfung weiter anhält, für wann rechnet die Bundesregierung mit deren Abschluss?
   b) In welchen „Arbeitsbereichen/Abteilungen“ wird der Themenkomplex beim BND bearbeitet?
   c) Wann und wem gegenüber werden die Ergebnisse des Berichts vollständig oder teilweise veröffentlicht?
   d) Inwiefern trifft es zu, dass die Arbeitsgruppe den Namen „PsyOps“ trug (SPIEGEL ONLINE vom 14. Januar 2017, „BND wirft Russland gezielte Stimmungsmache vor“)?
8. Mit welchen Maßnahmen will die Bundesregierung auf die Ergebnisse des Berichts reagieren, etwa um zu verhindern, dass die russische Regierung „mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“ (tagesschau.de vom 18. Februar 2016, „Russische Desinformation in Deutschland?“)?
9. Wann und von wem wurde die Bundesregierung durch die US-Regierung über Hackerangriffe von Sommer 2016 auf Server der Demokraten in den USA informiert, bei denen E-Mails des Parteivorstands sowie des Stabs von Hillary Clinton kopiert und an die Enthüllungsplattform Wikileaks weitergereicht wurden?
   a) Wann haben den Geheimdiensten der Bundesregierung erstmals Informationen vorgelegen, dass britische Geheimdienste bereits im Frühjahr 2015 durch überwachte Datenflüsse davon gewusst haben wollen, dass „Moskau“ die Server der Demokratischen Partei „gehackt“ habe (theguardian.com vom 7. Januar 2017, „UK intelligence gave US key tipoff about Russian hacking, report says“?
   b) Inwiefern hat die Bundesregierung bei ihrer auf Bundestagsdrucksache 18/10759 skizzierten Einschätzung der Vorfälle auch die Stellungnahme von ehemaligen US-Geheimdienstangehörigen geprüft, die eine russische Urheberschaft anzweifeln (http://gleft.de/1yH)?

c) Welche Beweise (nicht Annahmen oder Indizien) sind der Bundesregierung durch eingestufte oder nicht eingestufte Veröffentlichungen der US-Regierung zu den angeblichen russischen Hackerangriffen auf die Partei der Demokraten bekannt geworden?

10. Was ist der Bundesregierung über eine Spear-Phishing-Kampagne gegen Mitarbeiter von US-Regierung, Thinktanks und Nichtregierungsorganisationen bekannt, die dem US-Geheimdienstbericht zufolge am Wahlabend des 8. November 2016 begonnen hat?

11. Was ist der Bundesregierung aus eigenen Erkenntnissen oder der Verfolgung von Veröffentlichungen anderer über eine Instrumentalisierung der Enthüllungsplattform Wikileaks durch die russische Regierung bekannt?

12. Was ist der Bundesregierung darüber bekannt, dass US-amerikanische Geheimdienste die Computer russischer Stromversorger und Telekommunikationsanbieter sowie den Kreml „quasi vorbeugend“ mit „Cyber-Waffen“ infiltriert haben, um diese im Bedarfsfall zum Einsatz zu bringen (faz.net vom 9. Januar 2017, „Amerikas Geheimdienste munkeln“)?

13. Inwiefern ist auch die Bundesregierung der von US-Geheimdiensten geäußerten Ansicht (http://gleft.de/1yL), der russische Präsident habe eine „deutliche Präferenz“ für den Republikaner Donald Trump entwickelt und erwarte sich von ihm ähnlich gute Erfahrungen, wie er sie mit dem deutschen Ex-Bundeskanzler Gerhard Schröder (SPD) gemacht hat?

14. Von welchen weiteren Regierungen der Mitgliedstaaten der Europäischen Union oder der NATO erhielt die Bundesregierung Hinweise über eine vermeintlich russische „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“, und welche der Regierungen hat dafür auch Beweise mitteilen können?

15. Inwiefern wurden seit Beantwortung der Kleinen Anfragen auf Bundestagsdrucksachen 18/8631 und 18/10759 weiterhin keine Anwerbeversuche der „Mitarbeiter [deutscher] Parlamentarier oder politischer Stiftungen“ durch die russische Regierung festgestellt?

16. Was ist der Bundesregierung darüber bekannt, in wie vielen Fällen Einrichtungen der Europäischen Union im Jahr 2016 von Hackerangriffen betroffen waren und wie viele dieser Fälle einen geheimdienstlichen Ursprung haben?

17. Über wie viele mutmaßlich durch staatliche Stellen erfolgte „elektronische Angriffe gegen digitale Infrastrukturen der Bundesregierung“ wurde das BfV im gesamten Jahr 2016 durch das BSI unterrichtet, und wie viele davon wurden nach Prüfung durch das BfV tatsächlich Regierungen zugeordnet?

18. Welche Techniken klassifiziert das Bundesinnenministerium bei solchen Vorfällen als „hochspezialisierte Angriffe, die nur durch manuelle Analysen erkannt werden konnten“ (Bundestagsdrucksache 18/10759)?

19. Welche Angriffe auf deutsche Infrastrukturen werden vom BfV und BSI den Personen oder Gruppierungen „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ zugerechnet?

a) Welche Belege konnten die Ämter darüber zusammentragen, wer sich hinter den Kürzeln mutmasslich verbirgt?

b) Welche Daten sind bei Angriffen auf deutsche Infrastrukturen, die das BfV oder der BND „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ zurechnet, abgeflossen (bitte auch die Datenmenge benennen)?

c) Was ist der Bundesregierung darüber bekannt, inwiefern „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ in der Vergangenheit auch Ziele auf russischem Hoheitsgebiet angegriffen haben?

20. Worin besteht die „Vielzahl von Indizien“, wonach die Gruppe APT28 für die im Jahr 2015 versandten Cyber-Angriffe (Phishing-Mails) an Abgeordnete des Deutschen Bundestages versendet haben soll (Bundestagsdrucksache 18/10759)?

a) Welche Einrichtungen des Bundestages bzw. welche Abgeordnetenbüros waren von den Angriffen betroffen?

b) Welche Einrichtungen des Bundestages bzw. welche Abgeordnetenbüros öffneten die über Phishing-Mails verteilten URL und luden schließlich Schadsoftware aus dem Netz nach (sofern dies für die Bundesregierung nicht feststellbar war, bitte die Gründe mitteilen)?

c) Inwiefern könnten die am 8. Juni 2015 unter dem Absender „Angela Merkel“ versandten Phishing-Mails Informationen aus früheren Datenabflüssen genutzt haben, etwa zur Täuschung durch die angegebene bundestagsinterne URL „eudoxap01.bundestag.btg:8080/eudox/20150608-PDRInformationen.pdf“, hinter der sich im HTML-Code infizierte Server verbargen?

d) Welche Rückschlüsse lassen die Analysen der Bundesregierung auf die Gefährdung bestimmter Einrichtungen oder Büros von Abgeordneten durch zukünftige Angriffe zu?

e) Auf welche Weise hat die Bundesregierung die besonders gefährdeten Einrichtungen oder Büros von Abgeordneten über diese Risikoanalyse informiert?

21. Auf welche Weise werden die Überlegungen der Bundesregierung zum Umgang mit „Fake News“ weiterverfolgt (deutschlandfunk.de vom 9. Januar 2017, „In absehbarer Zeit werden Fake News die Wahl nicht entscheiden“?

22. Auf welche Weise werden die Überlegungen der Bundesregierung weiterverfolgt, die deutsche Spionageabwehr, wie vom Verfassungsschutzpräsidenten gefordert, mit „Gegenangriffen auf Cyberattacken“ reagieren zu lassen (tagesschau.de vom 10. Januar 2017, „Maaßen bläst zur Gegenattacke“)?

a) Welche Behörden sollten aus Sicht der Bundesregierung eine solche Möglichkeit erhalten?

b) Nach welcher Maßgabe müsste ein Urheber von Cyberangriffen als Adressat eines staatlichen Cyberangriffs zuvor zweifelsfrei festgestellt werden?

23. Wann soll die konkrete Einrichtung der „EU Hybrid Fusion Cell“ im geheimdienstlichen EU-Lagezentrum „EU Intelligence Analysis Centre“ des Europäischen Auswärtigen Dienstes erfolgen?

    a) Welche Details zur personellen Aufstellung sind der Bundesregierung mittlerweile bekannt?

    b) Wo soll die deutsche nationale Kontaktstelle für die „Hybrid Fusion Cell“ angesiedelt werden?

    c) Inwiefern ist die Abstimmung der „Hybrid Fusion Cell“ mit einer NATO-Abteilung gegen „hybride Bedrohungen“ zu gemeinsamen Übungen „auf politischer und technischer Ebene“ mittlerweile fortgeschritten, und welche Planungen sind der Bundesregierung dazu bekannt?

Berlin, den 17. Januar 2017

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333