Deutscher Bundestag **Drucksache 18/77**

18. Wahlperiode 20.11.2013

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Christine Buchholz, Annette Groth, Inge Höger, Ulla Jelpke, Stefan Liebich, Niema Movassat, Thomas Nord, Petra Pau, Dr. Petra Sitte, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.

Kooperationen zur sogenannten Cybersicherheit zwischen der Bundesregierung, der Europäischen Union und den Vereinigten Staaten

Trotz der Enthüllungen über die Spionage von britischen und US-Geheimdiensten in den Mitgliedstaaten der Europäischen Union existieren weiterhin eine Reihe von Kooperationen zu „Cybersicherheit“ zwischen den Regierungen. Hierzu zählt nicht nur die „Ad-hoc EU-US Working Group on Data Protection“, die eigentlich zur Aufklärung der Vorwürfe eingerichtet wurde, jedoch nach Auffassung der Fragesteller bislang ergebnislos verläuft. Schon länger existieren informelle Zusammenarbeitsformen, darunter die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ oder ein „EU-/US-Senior-Officials-Treffen“. Zu ihren Aufgaben gehört die Planung gemeinsamer ziviler oder militärischer „Cyberübungen“, in denen „cyberterroristische Anschläge“, über das Internet ausgeführte Angriffe auf kritische Infrastrukturen, „DDoS-Attacken“ sowie „politisch motivierte Cyberangriffe“ simuliert und beantwortet werden. Es werden auch „Sicherheitsinjektionen“ mit Schadsoftware vorgenommen. Eine dieser US-Übungen war „Cyberstorm III“ mit allen US-Behörden des Innern und des Militärs. Am „Cyber Storm III“ arbeiteten das „Department of Defense“, das „Defense Cyber Crime Center“, das „Office of the Joint Chiefs of Staff National Security Agency“, das „United States Cyber Command“ und das „United States Strategic Command“ mit. Während frühere „Cyberstorm“-Übungen noch unter den Mitgliedern der „Five Eyes“ (USA, Großbritannien, Australien, Kanada, Neuseeland) abgehalten wurden, nahmen an „Cyber Storm III“ auch Frankreich, Ungarn, Italien, Niederlande und Schweden teil. Seitens Deutschland waren das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) bei der zivil-militärischen Übung präsent – laut der Bundesregierung hätten die Behörden aber an einem „Strang“ partizipiert, wo keine militärischen Stellen anwesend gewesen sei (Bundestagsdrucksache 17/7578). Derzeit läuft in den USA die Übung „Cyberstorm IV“, an der Deutschland ebenfalls teilnimmt.

Auch in der Europäischen Union werden entsprechende Übungen abgehalten. „BOT12“ simuliert Angriffe durch „Botnetze“, „Cyber Europe 2010“ versammelte unter anderem die Computer Notfallteams CERT aus den Mitgliedstaaten. Nächstes Jahr ist eine „Cyber Europe 2014“ geplant. Derzeit errichtet die Europäische Union ein „Advanced Cyber Defence Centre“ (ACDC), an dem auch die Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., EADS Cassidian sowie der Internet-Knotenpunkt DE-CIX beteiligt sind.

Die Bundesregierung hat bestätigt, dass es weltweit bislang keinen „cyberterroristischen Anschlag“ gegeben hat (Bundestagsdrucksache 17/7578). Dennoch

werden Fähigkeiten zur entsprechenden Antwort darauf trainiert. Erneut wird also der „Kampf gegen den Terrorismus“ instrumentalisiert, diesmal um eigene Fähigkeiten zur Aufrüstung des Cyberspace zu entwickeln. Diese teils zivilen Kapazitäten können dann auch geheimdienstlich oder militärisch genutzt werden. Es kann angenommen werden, dass die Hersteller des kurz nach der Übung „Cyberstorm III“ auftauchenden Computerwurms „Stuxnet“ ebenfalls von derartigen Anstrengungen profitierten. Selbst die Bundesregierung bestätigt, dass sich „Stuxnet“ durch „höchste Professionalität mit den notwendigen personellen und finanziellen Ressourcen“ auszeichne und vermutlich einen geheimdienstlichen Hintergrund hat (Bundestagsdrucksache 17/7578).

Wir fragen die Bundesregierung:

1. Welche Konferenzen zu „Cybersicherheit“ haben auf der Ebene der Europäischen Union im Jahr 2013 stattgefunden (Bundestagsdrucksache 17/11969)?
   a) Welche Tagesordnung bzw. Zielsetzung hatten diese jeweils?
   b) Wer hat diese jeweils organisiert und vorbereitet?
   c) Welche weiteren Nicht-EU-Staaten waren daran mit welcher Zielsetzung beteiligt?
   d) Mit welchen Aufgaben oder Beiträgen waren auch Behörden der USA eingebunden?
   e) Mit welchem Personal waren deutsche öffentliche und private Einrichtungen beteiligt?
2. Inwieweit ist die enge und vertrauensvolle Zusammenarbeit deutscher Geheimdienste mit den Partnerdiensten Großbritanniens und der USA mittlerweile gestört, und welche Konsequenzen zieht die Bundesregierung daraus?
3. Welche Ergebnisse zeitigte der Prüfvorgang der Generalbundesanwaltschaft zur Spionage von Geheimdiensten befreundeter Staaten in Deutschland, und wann wurde mit welchem Ergebnis die Einleitung eines Ermittlungsverfahrens erwogen?
   a) Was hält das Bundesministerium der Justiz davon ab, ein Ermittlungsverfahren anzuordnen?
   b) Inwiefern kommt die Generalbundesanwaltschaft nach Ansicht der Bundesregierung in dieser Angelegenheit ihrer Verpflichtung nach, „Bedacht zu nehmen, dass die grundlegenden staatsschutzspezifischen kriminalpolitischen Ansichten der Regierung“ in die Strafverfolgungstätigkeit einfließen und umgesetzt werden (www.generalbundesanwalt.de zur rechtlichen Stellung des Generalbundesanwalts)?
4. Welche Abteilungen aus den Bereichen Innere Sicherheit, Informationstechnik sowie Strafverfolgung welcher Behörden der Europäischen Union nehmen mit welcher Personalstärke an der im Jahr 2010 gegründeten „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ (High-level EU-US Working Group on cyber security and cybercrime) teil (Bundestagsdrucksache 17/7578)?
   a) Welche Abteilungen des Bundesministeriums des Innern (BMI) und des BSI oder anderer Behörden sind in welcher Personalstärke an der Arbeitsgruppe bzw. Unterarbeitsgruppen beteiligt?
   b) Welche Ministerien, Behörden oder sonstigen Institutionen sind seitens der USA mit welchen Abteilungen an der Arbeitsgruppe bzw. an Unterarbeitsgruppen beteiligt?

5. Welche Sitzungen der „high-level EU-US Working Group on cyber security and cybercrime“ oder ihrer Unterarbeitsgruppen haben in den Jahren 2012 und 2013 mit welcher Tagesordnung stattgefunden?
6. Welche Inhalte eines „Fahrplans für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013“ hat die Arbeitsgruppe bereits entwickelt (Bundestagsdrucksache 17/7578)?
   a) Welche weiteren Angaben kann die Bundesregierung zur ersten dort geplanten Übung machen (bitte Teilnehmende, Zielsetzung und Verlauf umreißen)?
   b) Welche weiteren Übungen fanden statt oder sind geplant (bitte Teilnehmende, Zielsetzung und Verlauf umreißen)?
7. Inwiefern hat sich das „EU-/US-Senior-Officials-Treffen“ in den Jahren 2012 und 2013 auch mit den Themen „Cybersicherheit“, „Cyberkriminalität“ oder „Sichere Informationsnetzwerke“ befasst, und welche Inhalte standen hierzu jeweils auf der Tagesordnung?

   Sofern „Cybersicherheit“, „Cyberkriminalität“ oder „Sichere Informationsnetzwerke“, „Terrorismusbekämpfung und Sicherheit“, „PNR“, „Datenschutz“ auf der Tagesordnung standen, welchen Inhalt hatten die dort erörterten Themen?
8. Inwieweit trifft es nach Kenntnis der Bundesregierung zu, dass die Firma Booz Allen Hamilton für die in Deutschland stationierte US Air Force Geheimdienstinformationen analysiert (stern, 30. Oktober 2013)?
   a) Was ist der Bundesregierung darüber bekannt, dass die Firma Incadence Strategic Solutions für US-Einrichtungen in Stuttgart einen „hoch motivierten“ Mitarbeiter sucht, der „abgefangene Nachrichten sammeln, sortieren, scannen und analysieren“ soll?
   b) Welche Anstrengungen hat die Bundesregierung zur Aufklärung der Berichte unternommen, und welches Ergebnis wurde hierzu bislang erzielt?
9. Auf welche Weise, wem gegenüber und mit welchem Inhalt hat sich die Bundesregierung dafür eingesetzt, dass sich die „Ad-hoc EU-US Working Group on Data Protection“ umfassend mit den gegenüber den USA und Großbritannien im Sommer und Herbst 2013 bekannt gewordenen Vorwürfen der Cyberspionage auseinandersetzt (Bundestagsdrucksache 17/14739)?
10. Zu welchen offenen Fragen lieferte das Treffen der „Ad-Hoc EU-US-Arbeitsgruppe Datenschutz“ vom 6. November 2013 in Brüssel nach Kenntnis und Einschätzung der Bundesregierung keine konkreten Ergebnisse?
    a) Welche offenen Fragen sollen demnach schriftlich beantwortet werden, und welcher Zeithorizont ist hierfür angekündigt?
    b) Mit welchem Inhalt oder sogar Ergebnis wurden auf dem Treffen Fragen zur Art und Begrenzung der Datenerhebungen, zur Datenübermittlung, zur Datenspeicherung sowie US-Rechtsgrundlagen erörtert?
11. Innerhalb welcher zivilen oder militärischen „Cyberübungen“ oder vergleichbarer Aktivitäten haben welche deutschen Behörden in den letzten fünf Jahren „Sicherheitsinjektionen“ vorgenommen, bei denen Schadsoftware eingesetzt oder simuliert wurde, und worum handelte es sich dabei?
    a) Welche Programme wurden dabei „injiziert“?
    b) Wo wurden diese entwickelt, und wer war dafür jeweils verantwortlich?

12. Bei welchen Cyberübungen unter deutscher Beteiligung wurden seit dem Jahr 2010 Szenarien „geprobt“, die „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie „politisch motivierte Cyberangriffe“ zum Inhalt hatten, und um welche Szenarien handelte es sich dabei konkret (Bundestagsdrucksache 17/11341)?

13. Inwieweit bzw. mit welchem Inhalt oder konkreten Maßnahmen sind Behörden der Bundesregierung mit „Cyber Situation Awareness“ oder „Cyber Situation Prediction“ beschäftigt, bzw. welche Kapazitäten sollen hierfür entwickelt werden?

    a) Haben Behörden der Bundesregierung jemals von der Datensammlung „Global Data on Events, Location and Tone“ (GDELT) oder dem Dienst „Recorded Future“ Gebrauch gemacht?

    b) Falls ja, welche Behörden, auf welche Weise, und inwiefern hält die Praxis an?

14. Inwieweit treffen Zeitungsmeldungen (Guardian vom 1. November 2013, Süddeutsche Zeitung vom 1. November 2013) zu, wonach Geheimdienste Großbritanniens mit deren deutschen Partnern beraten hätten, wie Gesetzesbeschränkungen zum Abhören von Telekommunikation „umschifft“ oder anders ausgelegt werden könnten („The document also makes clear that British intelligence agencies were helping their German counterparts change or bypass laws that restricted their ability to use their advanced surveillance technology“; „making the case for reform“)?

    a) Inwieweit und bei welcher Gelegenheit haben sich deutsche und britische Dienste in den vergangenen zehn Jahren über die Existenz, Verabschiedung oder Auslegung entsprechender Gesetze ausgetauscht?

    b) Welche Kenntnis hat die Bundesregierung über ein als streng geheim deklariertes Papier des US-Geheimdienstes NSA aus dem Januar 2013, worin die Bundesregierung wegen ihres Umgangs mit dem G-10-Gesetz gelobt wird („Die deutsche Regierung hat ihre Auslegung des G-10-Gesetzes geändert, um dem BND mehr Flexibilität bei der Weitergabe geschützter Daten an ausländische Partner zu ermöglichen“, Nachrichtenmagazin DER SPIEGEL vom 1. November 2013)?

    c) Inwieweit trifft die dort gemachte Aussage (auch in etwaiger Unkenntnis des Papiers), nämlich dass der BND nun „flexibler“ bei der Weitergabe von Daten agiere, nach Einschätzung der Bundesregierung zu?

    d) Inwiefern lässt sich rekonstruieren, ob tatsächlich seit der Reform des G-10-Gesetzes in den Jahren 2008/2009 mehr bzw. weniger Daten an die USA oder Großbritannien übermittelt wurden, und was kann die Bundesregierung hierzu mitteilen?

15. Inwieweit trifft die Aussage des Nachrichtenmagazins „FAKT“ (11. November 2013) zu, wonach seitens des BND „der gesamte Datenverkehr [des Internets] per Gesetz zu Auslandskommunikation erklärt [wurde]“, da dieser „ständig über Ländergrenzen fließen würde“, und die Kommunikation dann vom BND abgehört werden könne, ohne sich an die Beschränkungen des G-10-Gesetzes zu halten?

16. Inwiefern sind Behörden der Bundesregierung im Austausch mit welchen Partnerbehörden der Mitgliedstaaten der Europäischen Union, der USA oder Großbritanniens hinsichtlich erwarteter „DDoS-Attacken“, die unter anderem unter den Twitter-Hashtags #OpNSA oder #OpPRISM besprochen werden?

    Inwiefern existieren gemeinsame Arbeitsgruppen oder fallbezogene, anhaltende Ermittlungen zu den beschriebenen Vorgängen?

17. Welche Regierungen von Mitgliedstaaten der Europäischen Union sowie anderer Länder sind bzw. waren nach Kenntnis der Bundesregierung am zivil-militärischen US-Manöver „Cyberstorm IV“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?

    a) Welches Ziel verfolgt „Cyberstorm IV“ im Allgemeinen, und inwiefern werden diese in zivilen, geheimdienstlichen und militärischen „Strängen“ unterschiedlich ausdefiniert?

    b) Wie ist das Verhältnis von zivilen zu staatlichen Akteuren bei Cyberstorm IV?

18. Welche US-Ministerien bzw. -Behörden sind bzw. waren nach Kenntnis der Bundesregierung an „Cyberstorm IV“ im Allgemeinen beteiligt?

    a) Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus der nach Auffassung der Fragesteller starken militärischen Beteiligung bei der „Cyberstorm IV“?

    b) Wie viele Angehörige welcher deutscher Behörden haben an welchen Standorten teilgenommen?

    c) Welche US-Ministerien bzw. -Behörden waren an „Cyberstorm IV“ an jenen „Strängen“ beteiligt, an denen auch deutsche Behörden teilnahmen?

19. Wie ist bzw. war die Übung nach Kenntnis der Bundesregierung strukturell angelegt, und welche Szenarien wurden durchgespielt?

    Wie viele Personen haben insgesamt an der Übung „Cyberstorm IV“ teilgenommen?

20. Worin bestanden die Aufgaben der 25 Mitarbeiter und Mitarbeiterinnen des BSI und des Mitarbeiters des BKA bei der Übung „Cyberstorm III“ (und falls ebenfalls zutreffend, auch bei „Cyberstorm IV), und wie haben sich diese eingebracht?

21. Inwieweit kann die Bundesregierung ausschließen, dass ihre Unterstützung der „Cyberstorm“-Übungen der USA dabei half, Kapazitäten zu entwickeln, die für digitale Angriffe oder auch Spionagetätigkeiten genutzt werden können, mithin die nun bekannt gewordenen US-Spähmaßnahmen auf die deutsche Beteiligung an entsprechenden Kooperationen zurückgeht?

22. Welche Kooperationen existieren zwischen dem BSI und den militärischen Behörden oder Geheimdiensten des Bundes?

23. Auf welche weitere Art und Weise wäre es möglich oder wird sogar praktiziert, dass militärische Behörden oder Geheimdienste des Bundes von Kapazitäten oder Forschungsergebnissen des BSI profitieren?

24. Welche Regierungen von Mitgliedstaaten der Europäischen Union oder anderer Länder sowie sonstige, private oder öffentliche Einrichtungen sind bzw. waren nach Kenntnis der Bundesregierung mit welchen Aufgaben am NATO-Manöver „Cyber Coalition 2013“ aktiv beteiligt, und welche hatten eine beobachtende Position inne (bitte auch die Behörden der Teilnehmenden aufführen)?

    a) Welches Ziel verfolgt „Cyber Coalition 2013“, und welche Szenarien wurden hierfür durchgespielt?

    b) Wer war für die Erstellung und Durchführung der Szenarien verantwortlich?

    c) An welchen Standorten fand die Übung statt, bzw. welche weiteren Einrichtungen außerhalb Estlands sind oder waren angeschlossen?

d) Wie hat sich die Bundesregierung in die Vor- und Nachbereitung von „Cyber Coalition 2013“ eingebracht?

25. Wann, mit welcher Tagesordnung, und mit welchem Ergebnis hat sich das deutsche „Cyberabwehrzentrum“ mit den bekannt gewordenen Spionagetätigkeiten Großbritanniens und der USA in Deutschland seit Juni 2013 befasst?

26. Wie viele Bedienstete von US-Behörden des Innern oder des Militärs sind an der Botschaft und den Generalkonsulaten in der Bundesrepublik Deutschland über die Diplomatenliste gemeldet, und welchen jeweiligen Diensten oder Abteilungen werden diese zugerechnet?

27. Worin besteht die Aufgabe der insgesamt zwölf Verbindungsbeamten und Verbindungsbeamtinnen des Department of Homeland Security (DHS), die beim Bundeskriminalamt akkreditiert sind (Bundestagsdrucksache 17/14474)?

28. Welche weiteren Inhalte der Konversation (außer zur „Bedeutung internationaler Datenschutzregeln“) kann die Bundesregierung zum „Arbeitsessen der Minister über transatlantische Themen“ beim Treffen der G6-Staaten mit US-Behörden hinsichtlich der Spionagetätigkeiten von US-Geheimdiensten „zur Analyse von Telekommunikations- und Internetdaten“ mitteilen (bitte ausführlicher angeben als in der Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 17/14833)?

29. Welche weiteren Angaben kann die Bundesregierung zur ersten und zweiten Teilfrage der Schriftlichen Frage 18 auf Bundestagsdrucksache 18/36 nach möglichen juristischen und diplomatischen Konsequenzen machen, da aus Sicht der Fragesteller der Kern der Fragen unberührt, mithin unbeantwortet bleibt?

a) Auf welche Weise wird hierzu „aktiv Sachverhaltsaufklärung“ betrieben, und welche Aktivitäten unternahmen welche Stellen der Bundesregierung hierzu?

b) Welche Erkenntnisse zur möglichen Überwachung der Redaktion des Nachrichtenmagazins „DER SPIEGEL“ bzw. ausländischer Mitarbeiter konnten dabei bislang gewonnen werden?

30. Worin bestand der „Warnhinweis“, den das Bundesamt für Verfassungsschutz (BfV) nach einem Bericht von „SPIEGEL ONLINE“ (10. November 2013) an die Länder geschickt hat?

a) Auf welche konkreten Quellen stützt das Amt seine Einschätzung einer „nicht auszuschließenden Emotionalisierung von Teilen der Bevölkerung“?

b) Welche Ereignisse hielt das BfV demnach für möglich oder sogar wahrscheinlich?

c) Welche Urheber/Urheberinnen hatte das BfV hierfür vermutet?

d) Inwiefern war die „Warnung“ mit dem BKA abgestimmt?

e) Aus welchem Grund wurde eine Frage des Leiters des rheinland-pfälzischen Verfassungsschutzes, Hans-Heinrich Preußinger, der sich ebenfalls nach dem „Warnhinweis“ erkundigte, nicht beantwortet?

f) Welche weiteren Landesregierungen haben ähnliche Anfragen gestellt, und in welcher Frist wurde ihnen wie geantwortet?

31. Auf welche Weise wird die Bundesregierung in Erfahrung bringen, ob die NSA im neuen US-Überwachungszentrum in Erbenheim bei Wiesbaden tätig ist (Bundestagsdrucksache 17/14739)?

32. Aus welchem Grund wurde die Kooperationsvereinbarung vom 28. April 2002 zwischen BND und NSA, u. a. bezüglich der Nutzung deutscher Überwachungseinrichtungen, wie in Bad Aibling, dem Parlamentarischen Kontrollgremium des Deutschen Bundestages erst elf Jahre später, am 20. August 2013, zur Einsichtnahme übermittelt (Bundestagsdrucksache 17/14739)?

33. Welches Ziel verfolgte die Übung „BOT12“, und wer nahm daran aktiv bzw. in beobachtender Position teil (Ratsdok. 5794/13, https://tem.li/mw1xt)?

    Wie wurden die dort behandelten Inhalte „test mitigation strategies and preparedness for loss of IT“ und „test Crisis Management Team“ nach Kenntnis der Bundesregierung nachträglich bewertet?

34. Auf welche Weise arbeiten Bundesbehörden oder andere deutsche Stellen mit dem ACDC auf europäischer Ebene zusammen?

    Welche Aufgaben übernehmen nach Kenntnis der Bundesregierung die ebenfalls beteiligte Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., das Unternehmen Cassidian sowie der Internet-Knotenpunkt DE-CIX?

35. Wofür wird im BKA derzeit eine „Entwickler/in bzw. Programmierer/in mit Schwerpunkt Analyse“ gesucht (http://tinyurl.com/myr948t)?

    a) Welche „Werkzeuge für die Analyse großer Datenmengen“ sowie zur „Operative[n] Analyse von polizeilichen Ermittlungsdaten“ sollen dabei entwickelt werden?

    b) Welche Funktionalitäten der „Datenaufbereitung, Zusammenführung und Bewertung“ soll die Software erfüllen?

    c) Auf welche Datenbanken soll nach derzeitigem Stand zugegriffen werden dürfen, und welche Veränderungen sind vom BKA hierzu anvisiert?

36. Welche weiteren, im Ratsdokument 5794/13 genannten Veranstaltungen beinhalteten nach Kenntnis der Bundesregierung Elemente zu „Cybersicherheit“?

    a) Wer nahm daran teil?

    b) Welchen Inhalt hatten die Übungen im Allgemeinen bzw. die Teile zu „Cybersicherheit“ im Besonderen?

37. Welche Treffen der „Friends of the Presidency Group on Cyber Issues“ haben nach Kenntnis der Bundesregierung im Jahr 2013 stattgefunden, wer nahm daran jeweils teil, und welche Tagesordnung wurde behandelt?

38. Welche Planungen existieren für eine Übung „Cyber Europe 2014“, und wer soll daran aktiv bzw. in beobachtender Position beteiligt sein?

    a) Wie soll die Übung angelegt sein, und welche Szenarien werden vorbereitet?

    b) Was ist der Bundesregierung darüber bekannt, inwiefern „Cyber Europe 2014“ als „dreilagige Übung“ angelegt und sowohl technisch, operationell und politisch tätig werden soll (www.enisa.europa.eu „Multilateral Mechanisms for Cyber Crisis Cooperations“)?

    c) Inwiefern soll hierfür auch der „Privatsektor“ eingebunden werden?

    d) Welche deutschen Behörden sollen nach jetzigem Stand an welchen Standorten an der „Cyber Europe 2014“ teilnehmen?

39. Welche Ergebnisse zeitigte das am 14. Juni 2013 veranstaltete „Krisengespräch“ mehrerer Bundesministerien mit Unternehmen und Verbänden der Internetwirtschaft für das Bundesinnenministerium, und welche weiteren Konsequenzen folgten daraus (Bundestagsdrucksache 17/14739)?

40. Inwieweit wurde das Umgehen von Verschlüsselungstechniken nach Kenntnis der Bundesregierung in internationalen Gremien oder Sitzungen multilateraler Standardisierungsgremien (insbesondere European Telecommunications Standards Institute – ETSI) thematisiert?

41. An welchen Sitzungen des ETSI oder anderer Gremien, an denen Bundesbehörden sich zum Thema austauschten, nahmen – soweit bekannt und erinnerlich – welche Vertreter/Vertreterinnen von US-Behörden oder Firmen teil?

42. Würde die Bundesregierung das Auftauchen von „Stuxnet“ mittlerweile als „cyberterroristischen Anschlag“ kategorisieren (Bundestagsdrucksache 17/7578)?

    a) Inwieweit liegen ihr mittlerweile „belastbare Erkenntnisse zur konkreten Urheberschaft“ von „Stuxnet“ vor?

    b) Inwiefern hält sie einen „nachrichtendienstlichen Hintergrund des Angriffs“ für weiterhin wahrscheinlich oder sogar belegt?

    c) Welche Anstrengungen hat sie in den Jahren 2012 und 2013 unternommen, um die Urheberschaft von „Stuxnet“ aufzuklären?

43. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat oder liegen ihr hierzu nach wie vor keine Informationen darüber vor, dass es eine derartige, nicht von Staaten ausgeübte versuchte oder erfolgreich ausgeführte Attacke jemals gegeben hat (Bundestagsdrucksache 17/7578)?

44. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2013 gegeben, die auf eine mutmaßliche oder nachgewiesene Urheberschaft von Nachrichtendiensten hindeuten, und um welche Angriffe bzw. Urheber handelt es sich dabei?

Berlin, den 18. November 2013

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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