

## **Antwort**

### **der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte,  
Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.  
– Drucksache 18/77 –**

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

#### Vorbemerkung der Fragesteller

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 (BKA) für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt 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“ versam-

melte 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).

1. Welche Konferenzen zu „Cybersicherheit“ haben auf der Ebene der Europäischen Union im Jahr 2013 stattgefunden (Bundestagsdrucksache 17/11969)?

Zu folgenden Konferenzen zu „Cybersicherheit“ im Jahr 2013 auf Ebene der Europäischen Union (d. h. Konferenzen, die von einer EU-Institution ausgerichtet wurden) liegen Kenntnisse vor:

Auftaktveranstaltung zum „Monat der europäischen Cybersicherheit“ (European Cyber Security Month – ECSM), 11. Oktober 2013, Brüssel.

- a) Welche Tagesordnung bzw. Zielsetzung hatten diese jeweils?

Die Konferenz war die offizielle Auftaktveranstaltung für die am „Monat der europäischen Cybersicherheit“ teilnehmenden Organisationen und Institutionen innerhalb der EU. Hierbei handelt es sich um eine europaweite Sensibilisierungskampagne zum Thema Internetsicherheit, die von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) gemeinsam mit der Europäischen Kommission durchgeführt wird. Ziel der Kampagne ist es, die Cybersicherheit unter den Bürgern zu fördern, deren Wahrnehmung von Cyberbedrohungen zu beeinflussen sowie aktuelle Sicherheitsinformationen durch Weiterbildung und Austausch von Good Practices zur Verfügung zu stellen. Die Tagesordnung der Konferenz ist auf der ENISA-Webseite abrufbar ([www.enisa.europa.eu/activities/identity-and-trust/whats-new/agenda](http://www.enisa.europa.eu/activities/identity-and-trust/whats-new/agenda)).

- b) Wer hat diese jeweils organisiert und vorbereitet?

Die Konferenz wurde gemeinsam von ENISA und der Europäischen Kommission organisiert und stand unter der Schirmherrschaft der litauischen EU-Ratspräsidentschaft.

- c) Welche weiteren Nicht-EU-Staaten waren daran mit welcher Zielsetzung beteiligt?
- d) Mit welchen Aufgaben oder Beiträgen waren auch Behörden der USA eingebunden?

Nach vorliegenden Kenntnissen waren keine Vertreter der USA bzw. von Nicht-EU-Mitgliedstaaten aktiv an der Konferenz beteiligt. Eine Teilnehmerliste liegt nicht vor.

- e) Mit welchem Personal waren deutsche öffentliche und private Einrichtungen beteiligt?

Deutschland war in Form jeweils eines Fachvortrages eines BSI-Vertreters sowie eines Vertreters des Vereins „Deutschland sicher im Netz e. V.“ an der Konferenz 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?

Die deutschen Nachrichtendienste arbeiten weiterhin im Rahmen ihrer gesetzlichen Aufgaben mit ausländischen Partnerdiensten zusammen.

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, „Bedenken zu nehmen, dass die grundlegenden staatschutzspezifischen kriminalpolitischen Ansichten der Regierung“ in die Strafverfolgungstätigkeit einfließen und umgesetzt werden ([www.generalbundesanwalt.de](http://www.generalbundesanwalt.de) zur rechtlichen Stellung des Generalbundesanwalts)?

Im Rahmen der Prüfvorgänge zu möglichen Abhörmaßnahmen US-amerikanischer und britischer Nachrichtendienste klärt der Generalbundesanwalt beim Bundesgerichtshof, ob ein in seine Zuständigkeit fallendes Ermittlungsverfahren einzuleiten ist. Hierbei berücksichtigt er die maßgeblichen Vorschriften der Strafprozessordnung.

Zu internen bewertenden Überlegungen des Generalbundesanwalts im Zusammenhang mit justizieller Entscheidungsfindung gibt die Bundesregierung keine Stellungnahme ab. Ebenso wenig sieht die Bundesregierung Veranlassung, auf die Tätigkeit des Generalbundesanwalts Einfluss zu nehmen.

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)?

Die Arbeiten in der „Arbeitsgruppe EU-USA zum Thema Cybersicherheit und Cyberkriminalität“ wurden unterteilt in vier Unterarbeitsgruppen: Public Private Partnerships, Cyber Incident Management, Awareness Raising und Cyber-Crime. An den Veranstaltungen der drei erstgenannten Unterarbeitsgruppen haben nach Kenntnis der Bundesregierung Mitarbeiter der Generaldirektion für Kommunikationsnetze, Inhalte und Technologien (GD Connect, CNECT) der Europäischen Kommission teilgenommen. Darüber hinaus nahmen vereinzelt Vertreter des Generalsekretariates des Rates, des Europäischen Auswärtigen Dienstes, der ENISA sowie des Joint Research Centre (JRC) teil.

- a) Welche Abteilungen des Bundesministeriums des Innern (BMI) und des BSI oder anderer Behörden sind in welcher Personalstärke an der Arbeitsgruppe bzw. Unterarbeitsgruppen beteiligt?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist jeweils themenorientiert mit insgesamt vier Mitarbeitern in den drei erstgenannten Unterarbeitsgruppen zu Cybersicherheit vertreten.

An der Unterarbeitsgruppe Cyber-Crime sind keine Vertreter des Bundesministeriums des Innern (BMI) und des BSI beteiligt. Anlassbezogen nahm das Bundeskriminalamt (BKA) zur Thematik „Bekämpfung der Kinderpornografie im Internet“ am 28. und 29. Juni 2011 an einer Sitzung dieser Unterarbeitsgruppe teil. Diese Veranstaltung wurde auf Initiative der „Expert Sub-Group on Cyber-crime“ im Auftrag der „EU-US Working Group On Cybersecurity and Cyber-crime“ durchgeführt.

- b) Welche Ministerien, Behörden oder sonstigen Institutionen sind seitens der USA mit welchen Abteilungen an der Arbeitsgruppe bzw. an Unterarbeitsgruppen beteiligt?

Die Arbeitsgruppe liegt in der Zuständigkeit der Europäischen Kommission. Der Bundesregierung liegen daher keine vollständigen Informationen darüber vor, wer von US-Seite beteiligt ist. Nach Kenntnis des BSI haben an den erstgenannten drei Unterarbeitsgruppen Mitarbeiter aus dem US-amerikanischen Heimatschutzministerium (Department of Homeland Security – DHS) teilgenommen, deren genaue Funktions- und Organisationszuordnung der Bundesregierung nicht bekannt ist.

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?

Nach Kenntnis der Bundesregierung haben folgende Sitzungen in den Jahren 2012 und 2013 stattgefunden:

Expert Sub-Group on Public Private Partnerships:

In dieser Unterarbeitsgruppe fanden eine Telefonbesprechung am 3. Mai 2012 sowie ein Workshop am 15. und 16. Oktober 2012 statt (EU-US Open Workshop on Cyber Security of ICS and Smart Grids).

Expert Sub-Group on Cyber Incident Management:

In dieser Unterarbeitsgruppe fand am 23. September 2013 ein Treffen statt. An dieser Sitzung nahm das BSI teil. Eine Tagesordnung gab es nicht.

Expert Sub-Group on Awareness Raising:

Im Rahmen dieser Unterarbeitsgruppe fand am 12. Juni 2012 eine Veranstaltung zum Thema „Involving Intermediaries in Cyber Security Awareness Raising“ statt.

Teilnehmer der High Level Group sind Vertreter der EU und der USA. Zu den Sitzungen hat die Bundesregierung mit Ausnahme des Treffens in Athen am Rande der 2. International Conference on Cyber-Crisis Cooperation and Exercises keine Informationen.

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)?

Es liegen keine Kenntnisse über Absprachen und Ergebnisse der Europäischen Union für weitere gemeinsame/abgestimmte transkontinentale Übungen vor.

- a) Welche weiteren Angaben kann die Bundesregierung zur ersten dort geplanten Übung machen (bitte Teilnehmende, Zielsetzung und Verlauf umreißen)?

Im November 2011 fand die Planbesprechung „CYBER ATLANTIC 2011“ statt, an der das BSI teilgenommen hat. An der Übung beteiligt waren IT-Sicherheitsexperten aus den für die Internetsicherheit zuständigen Behörden aus zahlreichen EU-Mitgliedstaaten sowie die entsprechenden „Pendants“ aus dem DHS. Thema der Übung waren Methoden und Verfahren der internationalen Zusammenarbeit zur Bewältigung schwerwiegender IT-Sicherheitsvorfälle und IT-Krisen. Es wurden zwei Szenarienstränge zu „fortschrittlichen Bedrohungen (APT)“ bzw. zu Ausfällen bei Prozesssteuerungssystemen diskutiert.

- b) Welche weiteren Übungen fanden statt oder sind geplant (bitte Teilnehmende, Zielsetzung und Verlauf umreißen)?

Es liegen der Bundesregierung keine Informationen zu weiteren geplanten Übungen vor.

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?

„EU-/US-Senior-Officials-Treffen“ werden von der Europäischen Union und den USA wahrgenommen. Am 24. und 25. Juli 2013 fand in Wilna ein EU-US Senior Officials Meeting zu Justiz-/Innenthemen statt. Dazu liegt der Bundesregierung der Ergebnisbericht („Outcome of Proceedings“) vor. Eine Unterrichtung seitens der Europäischen Union erfolgte am 11. September 2013 in der Ratsarbeitsgruppe JAIEX. Es wurden die Themen Datenschutz und Cybersicherheit/Cyberkriminalität angesprochen.

Laut Ergebnisbericht ist das Thema Datenschutz nur im Rahmen der nächsten Schritte zum Datenschutzpaket angesprochen worden sowie das Abkommen und dessen Zusammenspiel mit der Datenschutzgrundverordnung und der Richtlinie.

Zum Thema Cybersicherheit/Cyberkriminalität erläuterte die US-Delegation die neuen Richtlinien, die auf einer „Executive Order“ und einer „Presidential Policy Directive“ gründen. Zwei Hauptänderungen wurden hervorgehoben: Die Schlüsselrolle von privaten Akteuren und die Auffassung, dass eine Unterscheidung zwischen Cybersicherheit und Infrastrukturschutz nicht mehr möglich ist. Im Weiteren ist über den Stand und die nächsten Schritte der „EU-US Working Group on Cyber security and Cyber crime“ gesprochen worden.

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)?

Die Firma Booz Allen Hamilton ist für die in Deutschland stationierten Streitkräfte der Vereinigten Staaten von Amerika tätig. Grundlage dafür ist die deutsch-amerikanische Rahmenvereinbarung vom 29. Juni 2001 (geändert 2003 und 2005, BGBl. 2001 II S. 1018, 2003 II S. 1540, 2005 II S. 1115). Für jeden Auftrag wird ein Notenwechsel geschlossen, der im Bundesgesetzblatt veröffentlicht wird. Die Pflicht zur Achtung deutschen Rechts aus Artikel II des NATO-Truppenstatuts gilt auch für Unternehmen, die für die in der Bundesrepublik Deutschland stationierten Truppen der Vereinigten Staaten von Amerika tätig sind. Die Regierung der Vereinigten Staaten von Amerika ist verpflichtet, alle erforderlichen Maßnahmen zu treffen, um sicherzustellen, dass die beauftragten Unternehmen bei der Erbringung von Dienstleistungen das deutsche Recht achten. Der Geschäftsträger der Botschaft der Vereinigten Staaten von Amerika in Berlin hat dem Auswärtigen Amt auf Nachfrage am 2. August 2013 ergänzend schriftlich versichert, dass die Aktivitäten von Unternehmen, die von den Streitkräften der Vereinigten Staaten von Amerika in Deutschland beauftragt wurden, im Einklang mit allen anwendbaren Gesetzen und internationalen Vereinbarungen stehen.

- 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?

Ein Notenwechsel gemäß o. g. Rahmenvereinbarung zu der Firma Incadence Strategic Solutions wurde nicht geschlossen.

- b) Welche Anstrengungen hat die Bundesregierung zur Aufklärung der Berichte unternommen, und welches Ergebnis wurde hierzu bislang erzielt?

Siehe Antwort zu Frage 8a.

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)?

Die Bundesregierung hatte einen Vertreter in die „Ad-hoc EU-US Working Group on Data Protection“ entsandt. Die Ergebnisse der Arbeit der „Ad-hoc EU-US Working Group on Data Protection“ sind in dem Abschlussbericht vom 27. November 2013 festgehalten ([http://ec.europa.eu/justice/newsroom/data-protection/news/131127\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm)).

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?

Es wird auf den Abschlussbericht vom 27. November 2013 verwiesen (vgl. Antwort zu Frage 9).

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?

Für zivile Übungen werden grundsätzlich keine ausführbaren Schadprogramme entwickelt, die in operativen Netzen der Übenden eingesetzt („injiziert“) werden. Derartige „Schadprogramme“ werden in Deutschland im Rahmen der Übung in ihrer Funktionalität und Wirkung beschrieben, und es wird dann nur auf dieser Grundlage weitergeübt. Solche Beschreibungen sind regelmäßig Teil des Szenarios oder von Einlagen („injects“) jeder Cyber-übenden Behörde, die im Laufe der Übung an die Übungsspieler kommuniziert werden, um Aktionen auszulösen. Das BSI hat bei keiner Cyber-Übung „Sicherheitsinjektionen“ im Sinne eines physikalischen Einspielens von Schadprogrammen in Übungssysteme vorgenommen.

Die jährlich stattfindende NATO Cyber Defence-Übung „Cyber Coalition“ nutzt zur Überprüfung von Prozessen und Fähigkeiten im Rahmen des Schutzes der eigenen IT-Netzwerke marktverfügbare Schadsoftwaresimulationen. Dabei werden von Seiten der NATO-Planungsgruppe entsprechende Szenarien erarbeitet. Die Bundeswehr war an der Erarbeitung dieser Szenarien nicht beteiligt.

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)?

Bei den meisten Übungen spielt die Täterorientierung („cyberterroristische Anschläge“, „politisch motivierte Cyberangriffe“) keine Rolle, da es um die Koordination der Krisenmanagementmaßnahmen und die technische Problemlösung geht.

2010/2011:

Vorbemerkung:

Die jährlich stattfindende Cyber Defence Übungsserie „Cyber Coalition“ der NATO nutzt der aktuellen Bedrohungssituation angepasste Szenarien zur Simulation von IT-Angriffen auf das IT-System der NATO und der Übungsteilnehmer in unterschiedlichen Ausprägungen. Das für die Übung erstellte Übungshandbuch enthält auch Szenarien mit kritischen Infrastrukturen. Die Bundeswehr nimmt jedoch nur an Szenarien teil, die das IT-System der Bundeswehr unmit-

telbar betreffen. Bei der Cyber Defence Übung „Locked Shields“, die durch das Cooperative Cyber Defence Center of Excellence (CCDCoE) durchgeführt wird, werden in einer geschlossenen Testumgebung durch sogenannte Blue Teams verteidigte IT-Systeme durch Red Teams mit entsprechenden Werkzeugen und marktverfügbarer Schadsoftwaresimulation angegriffen.

- 2010, Bundessonderlage IT im Rahmen der LÜKEX 2009/10, Szenario: Störungen auf verschiedenen Ebenen der Internetkommunikation in Deutschland (OSI-Layer).
- EU CYBER EUROPE 2010, Szenario: Ausfall von fiktiven Internet-Hauptverbindungen zwischen den Teilnehmerländern.
- NATO CYBER COALITION 2010 (siehe Vorbemerkung)
- Cyberstorm III (Verweis auf die „VS-NfD“ eingestufte Anlage)\*
- EU EUROCYBEX. (Verweis auf die „VS-NfD“ eingestufte Anlage)\*
- LÜKEX 2011, Szenario: Länderübergreifendes IT-Krisenmanagement vor dem Hintergrund vielfältiger fiktiver IT-Angriffe auf kritische IT-Infrastrukturen in Deutschland. Konkret sah das Übungsszenario IT-Störungen vor, welche durch zielgerichtete elektronische Angriffe verursacht wurden und zu Beeinträchtigungen im Bereich von sowohl öffentlich als auch privat betriebenen Kritischen Infrastrukturen führten.
- EU-US CYBER ATLANTIC, Szenario: „Fortschrittliche Bedrohungen (APT)“ mit Verlust vertraulicher Daten und Ausfälle bei Prozesssteuerungssystemen.
- NATO CYBER COALITION 2011 (siehe Vorbemerkung)

2012

- LOCKED SHIELD 2012 des NATO Cooperative Cyber Defence Centre of Excellence (siehe Vorbemerkung)
- EU CYBER EUROPE 2012, Szenario: Abwehr von Distributed Denial of Service (DDoS), Angriffe einer fiktiven Angreifergruppe gegen verschiedene Online Angebote in den Teilnehmerländern, wie z. B. E-Government-Anwendungen und Online-Banking.
- NATO CYBER COALITION 2012 (siehe Vorbemerkung und Verweis auf die „VS-NfD“ eingestufte Anlage)\*

2013

- LOCKED SHIELD 2013 des NATO Cooperative Cyber Defence Centre of Excellence, (siehe Vorbemerkung)
- Cyberstorm IV (Verweis auf die „VS-NfD“ eingestufte Anlage)\*
- NATO CYBER COALITION 2013 (siehe Vorbemerkung)

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?

---

\* 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.



- 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?

Das BSI betreibt seit der Feststellung des Bedarfs im „Nationalen Plan zum Schutz von Informationsinfrastrukturen“ 2005 das IT-Lagezentrum mit dem Auftrag, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zu verfügen, um den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können. Darüber hinaus wurde im Jahr 2011 im Rahmen der Umsetzung der Cybersicherheitsstrategie für Deutschland das Nationale Cyberabwehrzentrum für den behördenübergreifenden Informationsaustausch zur Bedrohungslage und zur Koordinierung von Maßnahmen gegründet.

Im Rahmen seines gesetzlichen Auftrages führt das Amt für militärischen Abschirmdienst (MAD) in der Abschirmlage auch ein Lagebild hinsichtlich der gegen den Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) gerichteten IT-Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund.

Anlassbezogen werden die IT-Sicherheitsorganisationen der Bundeswehr, gegebenenfalls auch unmittelbar die entsprechend betroffenen Dienststellenleiter bzw. Funktionsträger, durch den MAD beraten und Sicherheitsempfehlungen ausgesprochen.

Es liegen keine Kenntnisse zu der in der Frage genannten Datensammlung bzw. des genannten Dienstes vor.

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 „umschiff“ 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“)?

Diese Meldungen treffen nicht zu.

- 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?

Im Rahmen der Zusammenarbeit zwischen dem Bundesnachrichtendienst (BND) und dem GCHQ finden und fanden zahlreiche Treffen statt. Bei einigen dieser Treffen wurde auch der Austausch von Ergebnissen aus der Fernmeldeaufklärung thematisiert. Darüber hinaus wurde durch den BND auf die Einhaltung der gesetzlichen Vorgaben (z. B. Artikel-10-Gesetz) hingewiesen. Das Bundesamt für Verfassungsschutz (BfV) hat zu den angesprochenen Themen keine Gespräche geführt.

- 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 Wei-

tergabe geschützter Daten an ausländische Partner zu ermöglichen“, Nachrichtenmagazin DER SPIEGEL vom 1. November 2013)?

Der Bundesregierung liegen hierzu keine über die Pressemeldungen hinausgehenden Erkenntnisse vor.

- 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?

Der BND agiert im Rahmen der gesetzlichen Vorschriften.

- 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?

Die Kooperation des BND mit anderen Nachrichtendiensten findet auf gesetzlicher Grundlage statt, insbesondere des BND- und Artikel-10-Gesetzes (G10). Im Rahmen des Artikel-10-Gesetzes fanden lediglich im Jahre 2012 in zwei Fällen Übermittlungen anlässlich eines derzeit noch laufenden Entführungsfalls an die NSA statt. Eine Übermittlung an den britischen Nachrichtendienst erfolgte nicht.

Für das BfV existiert zur der Zeit vor 2009 bzw. 2008 keine Übermittlungst Statistik, die die gewünschte Vergleichsbetrachtung ermöglichen würde. Allgemein ist darauf hinzuweisen, dass § 4 Absatz 4 G10, der Grundlage für die Übermittlung von G10-Erkenntnissen aus der Individualüberwachung des BfV ist, nur durch das Gesetz vom 31. Juli 2009 (BGBl. I S. 2499) geändert worden ist und zwar, indem in Nummer 1 Buchstabe a zusätzlich auf den neuen § 3 Absatz 1a verwiesen wird. Damit wurde gewährleistet, dass tatsächliche Anhaltspunkte für die Planung bzw. Begehung bestimmter Straftaten nach dem Kriegswaffenkontrollgesetz an die zur Verhinderung und Aufklärung dieser Taten zuständigen Stellen weitergegeben werden können. Die Erhebungsbefugnis des neuen § 3 Absatz 1a – in Bezug auf Telekommunikationsanschlüsse, die sich an Bord deutscher Schiffe außerhalb deutscher Hoheitsgewässer befinden – ist auf den BND beschränkt.

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?

Die Aussage trifft nicht zu und wird vom BND nicht vertreten.

Die Fernmeldeaufklärung in Deutschland erfolgt auf Grundlage einer G10-Anordnung unter Beachtung der Vorgaben von § 10 Absatz 4 G10 (geeignete Suchbegriffe, angeordnetes Zielgebiet, angeordnete Übertragungswege, angeordnete Kapazitätsbeschränkung). Eine Überwachung des gesamten Internetverkehrs durch den BND erfolgt dabei nicht.

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?

Nach Kenntnis der Bundesregierung gibt es hierzu keinen Austausch mit Partnerbehörden der EU-Mitgliedstaaten oder der USA.

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?

Deutschland war mit dem BSI an einem von der eigentlichen US-Übung getrennten, eigenständigen zivilen Strang von „Cyber Storm IV“ beteiligt. In diesem galt es, die internationale Zusammenarbeit im IT-Krisenfall zu verbessern. Übende Nationen waren hier neben Deutschland auch Australien, Kanada, Frankreich, Japan, die Niederlande, Norwegen, Schweden, Schweiz, Ungarn und die USA (Teile des US-CERT). Der Bundesregierung liegen nur Informationen zu dieser Teilübung vor. An dem Strang von „Cyber Storm IV“, an dem Deutschland beteiligt war, nahmen nur staatliche Akteure teil.

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“?

Deutschland war an einem von der eigentlichen US-Übung getrennten, eigenständigen zivilen Strang von „Cyber Storm IV“ beteiligt; deshalb kann keine Aussage zu möglichen Schlussfolgerungen und Konsequenzen aus einer militärischen Beteiligung gemacht werden.

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

Für das BSI haben ca. 40 Mitarbeiter am Standort Bonn teilgenommen.

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

An dem Strang von „Cyber Storm IV“, an dem Deutschland beteiligt war, nahm für die USA das DHS mit dem US-CERT teil.

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?

Die Übung war als verteilte „Stabsrahmenübung“ angelegt, bei der die jeweiligen Krisenstäbe oder Krisenreaktionszentren der Teilnehmerländer von ihren örtlichen Einrichtungen aus das internationale IT-Krisenmanagement übten (zusätzlich: Verweis auf die „VS-NfD“ eingestufte Anlage).\*

Der Bundesregierung liegen keine Zahlen vor, wie viele Personen in den jeweiligen Ländern teilgenommen haben.

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?

Das BSI hat bei beiden Übungen im Rahmen seiner Aufgabe als nationales IT-Krisenreaktionszentrum auf Basis der eingespielten Informationen Lagefeststellungen zusammengestellt und fiktive Maßnahmenempfehlungen für (simulierte) nationale Stellen in den Zielgruppen des BSI erstellt. Wesentlicher Fokus wurde auf den internationalen Informationsaustausch und die multinationale Zusammenarbeit gelegt. Bei „Cyberstorm IV“ wurde zusätzlich die 24/7-Schichtarbeit geübt. Bei beiden Übungen war das BSI in der Vorbereitung und lokalen Übungs- und Einlagensteuerung aktiv.

Bei der „Cyberstorm III“ hatte das BKA die Aufgabe, zu beraten, welche strafprozessualen Maßnahmen im Rahmen des Szenarios denkbar und erforderlich gewesen wären. Das BKA hat an der Übung „Cyber Storm IV“ nicht teilgenommen.

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?

An den Strängen von „Cyber Storm“, an denen deutsche Behörden beteiligt waren, wurden ausschließlich defensive Maßnahmen wie technische Analysen, organisatorische Empfehlungen und Maßnahmen bei der Bearbeitung von großen IT-Sicherheitsvorfällen geübt. Die Bundesregierung hat keine Erkenntnisse, die darauf schließen lassen, dass die Übungen Angriffskompetenzen hätten fördern können.

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

Der gesetzliche Auftrag des BSI als nationale, zivile IT-Sicherheitsbehörde besteht ausschließlich in der präventiven Förderung der Informations- und Cybersicherheit. Die Aufgabe des BSI ist die Förderung der Sicherheit in der Informa-

---

\* 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.

tionstechnik, insbesondere die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes. Gemäß seiner gesetzlichen Aufgabenstellung ist das BSI der zentrale IT-Sicherheitsdienstleister aller Behörden des Bundes. Dies schließt die Beratung der Bundeswehr in Fragen der präventiven IT-Sicherheit ein.

Im Bereich der Cybersicherheit findet eine regelmäßige Zusammenarbeit mit dem CERT der Bundeswehr (CERT-Bw) sowie der zugehörigen Fachaufsicht im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) zu IT-Sicherheitsvorfällen, zum IT-Krisenmanagement und bei Übungen statt. Des Weiteren unterstützt das BSI im Rahmen seines gesetzlichen Auftrages gemäß § 5 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSIG) das BfV, zum Beispiel zum Schutz der Regierernetze bei der Analyse nachrichtendienstlicher elektronischer Angriffe auf die Bundesverwaltung. Auf konkreten Anlass hin haben das BfV und der BND gemäß 3 BSIG zudem die Möglichkeit, an das BSI ein Ersuchen um Unterstützung zu stellen.

Darüber hinaus findet auf der Grundlage der Cyber-Sicherheitsstrategie für Deutschland innerhalb des Cyberabwehrzentrums eine Kooperation mit der Bundeswehr, dem MAD, dem BfV und dem BND statt. Das Cyber-Abwehrzentrum arbeitet unter Beibehaltung der Aufgaben und Zuständigkeiten der beteiligten Behörden auf kooperativer Basis und wirkt als Informationsdrehscheibe. Über eigene Befugnisse verfügt das Cyberabwehrzentrum nicht.

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?

Das BSI ist im Rahmen seines gesetzlichen Auftrags der zentrale IT-Sicherheitsdienstleister der gesamten Bundesverwaltung. Die Produkte und Dienstleistungen des BSI wie z. B. IT-Lageberichte, Warnmeldungen und IT-Sicherheitsempfehlungen werden grundsätzlich allen Behörden des Bundes zur Verfügung gestellt. Des Weiteren bietet das BSI eine IT-Sicherheitszertifizierung für IT-Produkte und -Systeme sowie eine Zulassung von IT-Komponenten für den Geheimschutz an. Da das BSI selbst keine Forschungsarbeit betreibt, sind Forschungsergebnisse folglich kein Bestandteil des BSI-Produktangebots.

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 auflisten)?

An der Übung „Cyber Coalition 2013“ (25. bis 29. November 2013) nahmen alle 28 NATO-Mitgliedstaaten sowie Österreich, Finnland, Irland, Schweden und die Schweiz teil. Neuseeland und die EU hatten Beobachterstatus (Quelle: [www.nato.int/cps/da/natolive/news\\_105205.htm](http://www.nato.int/cps/da/natolive/news_105205.htm)). Das BSI war in seiner Rolle als National Cyber Defense Authority (NCDA) gegenüber der NATO als zentrales Element des nationalen IT-Krisenmanagements aktiv.

Die Bundeswehr beteiligte sich mit BAAINBw (Standort Lahnstein), CERT-Bw (Standort Euskirchen), Betriebszentrum IT-System Bundeswehr (Standort Rheinbach) und CERT BWI (Standort Köln-Wahn) an der Übung (25. bis 29. November 2013). Diese Organisationselemente haben die Aufgabe, im

NATO-Kontext den Schutz des IT-Systems der Bundeswehr im Rahmen des Risiko- und IT-Krisenmanagements in der Bundeswehr sicherzustellen.

Das MAD-Amt nahm am Standort Köln teil. Der MAD hat im Rahmen der Übung die Aufgabe, nachrichtendienstliche Erkenntnisse an die zuständigen Vertreter der Bundeswehr zu übermitteln.

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

Ziel dieser Übung war die Anwendung von Verfahren der NATO im multinationalen Informationsaustausch. Es sollte das Incident Handling im Rahmen des Schutzes kritischer Informationsinfrastrukturen zur Eindämmung der Auswirkungen einer internationalen Cyber-Krise geübt werden. Aus den Übungserfahrungen heraus werden bestehende Verfahren harmonisiert und, wenn notwendig, neue Verfahren entwickelt. Die nationalen Übungsziele betrafen deutsche IT-Krisenmanagementprozesse mit der NATO sowie interne Verfahren und Prozesse.

Weitere Ausführungen sind der VS-NfD-Anlage zu entnehmen.\*

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

In verschiedenen Sitzungen der Vorbereitungsteams der teilnehmenden Nationen unter der Federführung der North Atlantic Treaty Organisation Computer Incident Response Capability (NATO-CIRC) wurden die Rahmenbedingungen für das Gesamtszenario sowie die Teilstränge vorgegeben. Für Deutschland waren das BSI, das BAAINBw und das CERT-Bw beteiligt.

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

An den Strängen, an denen Deutschland teilnahm, waren neben der zentralen Übungssteuerung in Tartu in Estland, das BSI in Bonn, das BAAIN-Bw in Koblenz, das CERT-Bw in Euskirchen sowie das Betriebszentrum IT-System der Bundeswehr in Rheinbach beteiligt. Weitere Informationen liegen nicht vor.

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

Hierzu wird auf die Antwort zu Frage 24b verwiesen.

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?

Die Thematik war Bestandteil der täglichen Lagebeobachtung durch das Cyberabwehrzentrum.

26. Wie viele Bedienstete von US-Behörden des Innern oder des Militärs sind an der Botschaft und den Generalkonsulaten in der Bundesrepublik

---

\* 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.

Deutschland über die Diplomatenliste gemeldet, und welchen jeweiligen Diensten oder Abteilungen werden diese zugerechnet?

Der Bundesregierung liegen keine Angaben vor, wie viele entsandte Bedienstete der hier akkreditierten US-Missionen den US-Behörden des Innern zuzurechnen sind. Entsprechend den Bestimmungen des Wiener Übereinkommens über Diplomatische Beziehungen wird das Personal beim Militärattachéstab separat erfasst, da für den Militärattaché ein gesondertes Akkreditierungsverfahren vorgesehen ist.

Bei der US-Botschaft in Berlin sind zurzeit 155 Entsandte angemeldet, davon 92 zur Diplomatenliste (Rest entsandtes verwaltungstechnisches Personal). Hier von sind sieben Diplomaten dem Militärattachéstab zugeordnet, weitere drei dem „Office of Defense Cooperation“ (Wehrtechnik).

Nachfolgend die Zahlen für die US-Generalkonsulate:

- Außenstelle Bonn: zwei Entsandte, beide „Office of Defense Cooperation“ (Wehrtechnik),
- Düsseldorf: zwei Entsandte, beide zur Konsularliste angemeldet,
- Frankfurt: 428 Entsandte, davon 28 zur Konsularliste angemeldet (Rest entsandtes verwaltungstechnisches Personal). Die hohe Zahl an verwaltungstechnischem Personal erklärt sich aus der Tatsache, dass von dort aus Verwaltungstätigkeiten (z. B. Logistikerunterstützung, Beschaffungen, Transportwesen, Wartung und Instandhaltung) mit regionaler und teilweise überregionaler Zuständigkeit für alle US-Vertretungen in Deutschland und Europa wahrgenommen werden. Entsprechend ist der Anteil an verwaltungstechnischem Personal an den anderen US-Vertretungen in Deutschland geringer.
- Hamburg: sechs Entsandte, davon einer zur Konsularliste angemeldet (Rest entsandtes verwaltungstechnisches Personal),
- Leipzig: zwei Entsandte, beide zur Konsularliste angemeldet,
- München: 26 Entsandte, davon 13 zur Konsularliste angemeldet (Rest entsandtes verwaltungstechnisches Personal).

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)?

Beim BKA sind derzeit lediglich sechs Verbindungsbeamte (VB) der US-Einwanderungs- und Zollbehörde (Immigration Customs Enforcement“ – ICE), welche dem DHS unterstellt ist, gemeldet. Irrtümlich war in der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 17/14474 vom 1. August 2013 angegeben, dass zwölf VB gemeldet seien. Die VB verrichten ihren Dienst im US-amerikanischen Generalkonsulat Frankfurt/Main.

Das ICE befasst sich mit Einwanderungs- sowie Zollstraftaten.

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)?

Bei dem Arbeitsessen sagte US-Justizminister Eric Holder ferner zu, sich für eine weitere Aufklärung der Sachverhalte einzusetzen.

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?
- Auf welche Weise wird hierzu „aktiv Sachverhaltsaufklärung“ betrieben, und welche Aktivitäten unternahm welche Stellen der Bundesregierung hierzu?
  - Welche Erkenntnisse zur möglichen Überwachung der Redaktion des Nachrichtenmagazins „DER SPIEGEL“ bzw. ausländischer Mitarbeiter konnten dabei bislang gewonnen werden?

Die Bundesregierung prüft die einzelnen Vorwürfe, beispielsweise durch die im BfV eingerichtete Sonderauswertung „Technische Aufklärung durch US-amerikanische, britische und französische Nachrichtendienste mit Bezug zu Deutschland“. Zu möglichen Konsequenzen kann die Bundesregierung erst Stellung nehmen, wenn ein konkreter Sachverhalt vorliegt.

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?
- Auf welche konkreten Quellen stützt das Amt seine Einschätzung einer „nicht auszuschließenden Emotionalisierung von Teilen der Bevölkerung“?
  - Welche Ereignisse hielt das BfV demnach für möglich oder sogar wahrscheinlich?
  - Welche Urheber/Urheberinnen hatte das BfV hierfür vermutet?
  - Inwiefern war die „Warnung“ mit dem BKA abgestimmt?
  - Aus welchem Grund wurde eine Frage des Leiters des rheinland-pfälzischen Verfassungsschutzes, Hans-Heinrich Preußinger, der sich ebenfalls nach dem „Warnhinweis“ erkundigte, nicht beantwortet?
  - Welche weiteren Landesregierungen haben ähnliche Anfragen gestellt, und in welcher Frist wurde ihnen wie geantwortet?

Vor dem Hintergrund der Berichterstattung und der intensiv geführten Diskussionen über NSA-Abhörmaßnahmen erschien eine abstrakte Gefährdung US-amerikanischer Einrichtungen nicht ausgeschlossen. Das genannte Schreiben diente rein präventiv dazu, bezüglich dieser Situation zu sensibilisieren. Es lagen aber keine Erkenntnisse hinsichtlich einer konkreten Gefährdung US-amerikanischer Einrichtungen und Interessen in Deutschland vor.

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)?

Die US-Streitkräfte sind im Infrastrukturverfahren nach dem Verwaltungsabkommen Auftragsbautengrundsätze ABG 1975 nicht gehalten, Aussagen über



den oder die Nutzer eines geplanten Bauprojektes gegenüber Deutschland zu treffen.

Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 46 bis 49 auf Bundestagsdrucksache 17/14739 sowie auf die Antwort der Bundesregierung zu Frage 32 auf Bundestagsdrucksache 17/14560 verwiesen.

Das BfV wird die Frage einer etwaigen Präsenz der NSA in Erbenheim zunächst im Rahmen der bestehenden Kontakte zu US-Diensten klären.

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)?

Die im Jahr 2002 vorgeschriebene Unterrichtungspflicht der Bundesregierung gegenüber dem Parlamentarischen Kontrollgremium (PKGr) ergab sich bis zum Jahr 2009 aus § 2 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) a. F. Der Wortlaut der Regelung deckt sich mit der seit 2009 geltenden Bestimmung in § 4 Absatz 1: „Die Bundesregierung unterrichtet das Parlamentarische Kontrollgremium umfassend über die allgemeine Tätigkeit der in § 1 Absatz 1 genannten Behörden und über Vorgänge besonderer Bedeutung. Auf Verlangen des PKGr hat die Bundesregierung auch über sonstige Vorgänge zu berichten.“ Das Gesetz schreibt nicht vor, in welcher Art und Weise diese Unterrichtung erfolgt.

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?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

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 beteiligten Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., das Unternehmen Cassidian sowie der Internet-Knotenpunkt DE-CIX?

Nach Kenntnis der Bundesregierung arbeiten keine Bundesbehörden mit dem ACDC zusammen.

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?

Die Stelle ist für Serviceaufgaben im Bereich der operativen Analyse ausgeschrieben. Dort werden die Ermittlungsreferate bei der Auswertung von digitalen Daten unterstützt, die im Rahmen von Ermittlungsverfahren erhoben wurden. Ziel ist nicht die Entwicklung einer bestimmten Software, sondern die anlassbezogene Schaffung von Lösungen für Datenaufbereitungs- und Darstellungsprobleme.

Die im Einzelfall zu analysierenden Daten stammen aus operativen Maßnahmen. Falls erforderlich, kann ein Datenabgleich mit Daten aus den polizeilichen Informationssystemen INPOL und b-case erfolgen.

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

Im Ratsdokument 5794/13 werden folgende Übungen genannt, die nach Kenntnis der Bundesregierung Elemente zu „Cybersicherheit“ beinhalten:

- Cyber Europe 2014,
- EuroSOPEX series of exercises,
- Personal Data Breach EU Exercise.

- a) Wer nahm daran teil?

Cyber-Europe 2014: Auf die Antwort zu Frage 38 wird verwiesen

EuroSOPEX series of exercise: Es liegen der Bundesregierung hierzu keine Informationen vor.

Personal Data Breach EU Exercise: Es liegen der Bundesregierung hierzu keine Informationen vor.

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

Cyber-Europe 2014: Auf die Antwort zu Frage 38 wird verwiesen.

EuroSOPEX series of exercise: In dieser Übungsserie, organisiert von ENISA, geht es um die nationale und multinationale Anwendung der Europäischen Standard Operating Procedures (SOP) (Verfahren zur Reaktion auf IT-Krisen mit einer europäischen Dimension).

Personal Data Breach EU Exercise: Es liegen der Bundesregierung hierzu keine Informationen vor.

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?

Die folgenden Treffen der „Friends of the Presidency Group on Cyber Issues“ (Cyber-FoP) haben nach Kenntnis der Bundesregierung im Jahr 2013 stattgefunden (die jeweilige Agenda ist als Anlage beigefügt – auch abrufbar unter <http://register.consilium.europa.eu/servlet/driver?typ=&page=Simple&lang=EN>):

- 25. Februar 2013 (CM 1626/13),

- 15. Mai 2013 (CM 2644/13),
- 3. Juni 2013 (CM 3098/13),
- 15. Juli 2013 (CM 3581/13),
- 30. Oktober 2013 (CM 4361/1/13),
- 3. Dezember 2013 (CM 5398/13).

An den Sitzungen nehmen regelmäßig Vertreter vom Bundesministerium des Innern und des Auswärtigen Amts sowie anlassbezogen Vertreter weiterer Ressorts wie des Bundesministeriums der Finanzen oder des Bundesministeriums für Wirtschaft und Technologie teil.

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

Die Übungsserie „Cyber Europe 2014“ befindet sich in Vorbereitung. Zur Teilnahme eingeladen werden nach jetzigem Kenntnisstand Behörden aus dem IT-Sicherheits-Umfeld der EU-Mitgliedstaaten, das CERT-EU sowie die EFTA-Partner. Es liegen keine Kenntnisse über Einladungen anderer Staaten und/oder Organisationen vor.

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

Die Übung wird voraussichtlich dreigeteilt mit einem übergreifenden Gesamtszenario angelegt.

Dabei soll in drei Teilübungen jeweils ein Aspekt der Zusammenarbeit

- der technischen CERT-Arbeitsebene (technische Analysten) oder
- der jeweiligen IT-Krisenstäbe oder Krisenreaktionszentren der Teilnehmerländer von ihren örtlichen Einrichtungen aus als verteilte „Stabsrahmenübung“ oder
- der ministeriellen Ebene für politische Entscheidungen geübt werden.

Die Abstimmung der Mitgliedstaaten für das Szenario ist noch nicht abgeschlossen.

- 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](http://www.enisa.europa.eu) „Multilateral Mechanisms for Cyber Crisis Cooperations“)?

Auf die Antwort zu Frage 38a wird verwiesen.

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

Es ist geplant, mindestens für die operationelle, ggf. auch die technische Teilübung den „Privatsektor“ in Form einzelner nationaler Unternehmen der Kritischen Infrastrukturen einzubinden.

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

An der „Cyber Europe 2014“ sollen nach jetzigem Stand das BSI und die Bundesnetzagentur 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)?

Wie in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 12. September 2013 (Bundestagsdrucksache 17/14739) bereits dargestellt wurde, erfolgte das informelle Gespräch auf eine kurzfristige Einladung des Bundesministeriums für Wirtschaft und Technologie. Es sollte vor allem einem frühen Meinungs- und Informationsaustausch dienen. Konkrete Ergebnisse oder Schlussfolgerungen waren nicht zu erwarten. Die beteiligten Wirtschaftskreise konnten zu diesem Zeitpunkt noch keine weiterführenden Erkenntnisse liefern.

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?

Der Bundesregierung liegen hierzu keine Kenntnisse vor.

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?

Die Bundesregierung wertet den Fall „Stuxnet“ nicht als „cyberterroristischen Anschlag“, sondern als einen Fall von Cyber-Sabotage auf Kritische Infrastrukturen. Es liegen keine belastbaren Erkenntnisse zur konkreten Urheberschaft vor. Aufgrund der Komplexität des Schadprogramms, der Auswahl des Angriffsziels sowie der für den Angriff erforderlichen erheblichen technischen, personellen und finanziellen Ressourcen wird weiterhin von einem nachrichtendienstlichen Hintergrund ausgegangen.

Die zu „Stuxnet“ vorliegenden Erkenntnisse sind durch das BfV hinsichtlich einer möglichen nachrichtendienstlichen Urheberschaft bewertet worden.

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)?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Anfrage vor.

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

Im Jahr 2013 wurde erneut eine Vielzahl „elektronischer Angriffe“, überwiegend durch mit Schadcodes versehene E-Mails, auf das Regierungsnetz des Bundes festgestellt. Dabei steht in der Regel das Interesse an politisch sensiblen Informationen im Vordergrund. Die gezielte Vorgehensweise und die Zielauswahl selbst gehören zu wichtigen Indizien für eine nachrichtendienstliche Steuerung der Angriffe, die verschiedenen Staaten zugerechnet werden.

Die IT-Systeme des zum BMVg gehörenden Geschäftsbereichs waren 2013 Ziel von IT-Angriffen in diversen Formen. Die Einbringung von Schadsoftware in die IT-Netze erfolgte hierbei sowohl durch mobile Datenträger als auch über das Internet. Hinsichtlich der Angriffe über das Internet ergaben sich in einzelnen Fällen Hinweise auf nachrichtendienstlich gesteuerte, zielgerichtete Angriffe mit chinesischem Bezug.





