Deutscher Bundestag **Drucksache 17/10379**

17. Wahlperiode 24. 07. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Herbert Behrens, Sevim Dağdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/10271 –

Repression gegen Jugendliche wegen virtueller Proteste gegen die GEMA

Vorbemerkung der Fragesteller

Im Juni 2012 hatte das Bundeskriminalamt (BKA) laut mehrerer Medienberichte die Wohnungen von über 100 Personen durchsucht und Computer und andere Ausrüstung (z. B. externe Festplatten, Kartenlesegeräte, Mobiltelefone, Playstations) beschlagnahmt. Ihnen wird vorgeworfen, an einer virtuellen Protestaktion gegen die Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) teilgenommen zu haben. Die Website der GEMA wurde hierfür am Abend des 17. Dezember 2011 von den Demonstranten mit Denial-of-Service-Anfragen (DoS) besucht. Angeblich sei die Website der GEMA aber zu keinem Zeitpunkt unerreichbar gewesen.

Offensichtlich hatte ein Nutzer namens „AnonLulz“ zum Protest aufgerufen. Die Razzien richteten sich demzufolge gegen vermeintliche Mitglieder oder Sympathisanten des Hackerkollektivs „Anonymous“, schreibt „WELT ONLINE“ am 13. Juni 2012. Dies habe ein Sprecher der Generalstaatsanwaltschaft Frankfurt bestätigt. Hackerangriffe sei die GEMA gewohnt, berichtet „WELT ONLINE“ weiter. Laut „SPIEGEL ONLINE“ (13. Juni 2012) werfen die Behörden den Verdächtigen Computersabotage (§ 303b des Strafgesetzbuchs – StGB) vor, was mit einer mehrjährigen Freiheitsstrafe geahndet werden kann. Die Ermittlungen hierzu leitet die Generalstaatsanwaltschaft Frankfurt mit Unterstützung des Bundeskriminalamts.

Nach Ansicht der Fragesteller/Fragestellerinnen handelt es sich bei der inkriminierten Aktion weder um einen Hackerangriff noch um Computersabotage, wonach gegen die Verdächtigen ermittelt wird. Die Protestierenden nutzten ein Programm (Low Orbit Ion Cannon – LOIC), das über den Dienst PasteHTML im Internet bereitgestellt wurde. Teilnehmer an der Aktion mussten hierfür lediglich einen Mausklick auf der Website von PasteHTML vornehmen. Vielmehr handelt es sich um eine Protestaktion, die Kriterien einer Onlinedemonstration erfüllt. Die GEMA protokollierte aber die IP-Adressen der Demonstranten und übergab diese Polizeibehörden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 20. Juli 2012 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

„SPIEGEL ONLINE“ berichtet weiter, dass es sich bei den Verdächtigen eher um Jugendliche und Heranwachsende handele, nicht aber um die Anschlussinhaber, gegen die sich die Durchsuchungsbeschlüsse richteten. Teilweise hätten die Betroffenen aber auch keine Ahnung, wer die Geräte bzw. IP-Adressen genutzt haben könnte. Das „Handelsblatt“ gibt die Staatsanwaltschaft überdies mit dem Zitat wieder, es seien „überwiegend Mitläufer“ festgenommen worden (Onlineausgabe, 14. Juni 2012). Das Ziel der hundertfachen Durchsuchungen sei eine „heilsame Schockwirkung“. Viele würden mit einer Ermahnung und Auflagen wie Sozialstunden davonkommen. Ob weitere zwangspädagogische Maßnahmen folgen ist unklar: Am 15. Juni 2012 hatte die GEMA laut der „Mitteldeutsche Zeitung“ (Meldung von dapd, Onlineausgabe MZ, 15. Juni 2012) erneut eine Strafanzeige gestellt, da neuerliche Proteste verzeichnet wurden. Laut der GEMA-Sprecherin Ursula Goebel habe die Gesellschaft „deshalb eine neue Strafanzeige gestellt und die Daten der Angreifer an das BKA weitergeleitet“. Laut einem Bericht von heise.de (19. Juni 2012) habe die GEMA jedoch keine IP-Adressen aufzeichnen können.

Nach Ansicht der Fragesteller/Fragestellerinnen sollen die übertriebenen Repressalien eine Symbolwirkung entfalten, um derartige Proteste zukünftig zu unterbinden. Allerdings wird zu wenig gewürdigt, dass es sich dabei um eine virtuelle Versammlung handelt, deren Schutzwürdigkeit unter dem Versammlungsrecht geprüft werden muss.

1. Welche Bundes- und – nach Kenntnis der Bundesregierung – Landesbehörden sind seit wann an den Ermittlungen wegen Störungen der GEMA-Website beteiligt, und von wem wurden diese geleitet?

   Welche Rolle haben in diesem Zusammenhang das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt (BKA), das Zollkriminalamt und die Bundespolizei übernommen?

Das Bundeskriminalamt (BKA) ermittelte seit dem 13. Dezember 2011 unter Sachleitung der Generalstaatsanwaltschaft Frankfurt/Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) wegen des Verdachts der Computersabotage zum Nachteil der GEMA. Die Ermittlungstätigkeiten des BKA umfassten die Einholung von Bestandsdatenauskünften gemäß § 113 des Telekommunikationsgesetzes (TKG) zu den in Rede stehenden IP-Adressen und die Aufbereitung des Ermittlungskomplexes zur Abgabe an die zuständigen Landesdienststellen. Nach Abschluss dieser Ermittlungen beim BKA am 12. April 2012 wurden die Verfahren durch die ZIT an die jeweils zuständigen Staatsanwaltschaften in 14 Bundesländern zur weiteren Bearbeitung und Ermittlung abgegeben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Zollkriminalamt (ZKA) und die Bundespolizei (BPOL) waren zu keiner Zeit in die Ermittlungen eingebunden.

2. Gegen wie viele Verdächtige werden nach Kenntnis der Bundesregierung in diesem Zusammenhang Ermittlungsverfahren geführt?

Die Ermittlungen richteten sich gegen Anschlussinhaber von 106 IP-Adressen.

   a) Wie viele Beschuldigte wurden in diesem Zusammenhang jeweils mit welchen Zwangsmaßnahmen aufgesucht?

Das BKA hat in keinem der 106 Fälle Durchsuchungsmaßnahmen durchgeführt. Ob und welche strafprozessualen Maßnahmen im Einzelfall durchgeführt wurden, oblag der örtlich zuständigen Staatsanwaltschaft/Dienststelle. Im Übrigen liegen der Bundesregierung keine über die Antworten zu den Fragen 1 und 2a

hinausgehenden Erkenntnisse über die in der Zuständigkeit der betroffenen Länder geführten Verfahren vor.

b) In welchen Bundesländern wurden wie viele Durchsuchungen durchgeführt?

Der Bundesregierung liegen keine über die Antworten zu den Fragen 1 und 2a hinausgehenden Erkenntnisse über die in der Zuständigkeit der betroffenen Länder geführten Verfahren vor.

c) Trifft es zu, dass sich die Zwangsmaßnahmen vielfach gegen Anschlussinhaber richteten, diese aber offensichtlich nicht selbst an den Protesten teilnahmen, sondern stattdessen gegen „Jugendliche und Heranwachsende“ (stern, Onlineausgabe, 14. Juni 2012)?

Auf die Antwort zu Frage 2b wird verwiesen.

3. Trifft es zu, dass die von der GEMA „ausgelieferten“ IP-Adressen von Verdächtigen über einen Link bei PasteHTML auf die GEMA-Website gelangt waren?

   a) Falls nein, auf welche Weise sollen die Verdächtigen die GEMA-Website sonst „attackiert“ haben?

   b) In welchem Maße sind laut den Ermittlungen Werkzeuge zum Generieren wiederholter Besuche der GEMA-Website genutzt worden (z. B. auch Add ons für Browser)?

   c) Inwieweit kamen auch automatisierte Javascripts zur Anwendung?

Im Rahmen der Ermittlungen konnte festgestellt werden, dass ein webbasiertes LOIC (Low Orbit Ion Cannon) für den Angriff genutzt wurde. Dabei nutzen die Teilnehmer der Distributed Denial of Service Attack (DDoS-Attacke) die Pastehtml-Webseite. Um den Angriff auszulösen, ist die aktive Betätigung des in diesem Fall mit „Feuer Frei“ benannten Buttons erforderlich. Dadurch wird ein „Angriffsscript“ (Java-Script) an den anfragenden Computer des selbst aktiv handelnden Teilnehmers übertragen, das durch den Browser des Aufrufers interpretiert und ausgeführt wird. Daraufhin erfolgen die massenhaften Anfragen (DDoS-Attacke) durch den Computer des Teilnehmers (nicht durch die Pastehtml-Seite) auf die „anzugreifende Webseite“. Weitere für die DDoS-Attacke genutzte Tools wurden nicht festgestellt.

4. Welche Technik wurde bei den Razzien durch das BKA und – nach Kenntnis der Bundesregierung – durch die Generalstaatsanwaltschaft oder weitere beteiligte Polizeien konkret beschlagnahmt?

   a) Trifft es zu, dass auch Router, externe Festplatten, Kartenlesegeräte, Mobiltelefone und Playstations mitgenommen wurden?

   b) Falls ja, wie viele?

   c) Falls ja, inwiefern soll deren forensische Auswertung Rückschlüsse auf ein Teilnahme an den GEMA-Protesten liefern?

   d) Welche Erkenntnisse erhoffen sich die Ermittlungsbehörden durch die Beschlagnahme oder Untersuchung von Playstations?

   e) Nach welchem Zeitraum wurden die Geräte ihren Besitzern/Besitzerinnen wieder ausgehändigt?

   f) Welche Geräte werden immer noch und aus welchen Gründen einbehalten?

Der Bundesregierung liegen keine über die Antworten zu den Fragen 1 und 2a hinausgehenden Erkenntnisse über die in der Zuständigkeit der betroffenen Länder geführten Verfahren vor.

5. Welche Praxis existiert bei Bundesbehörden hinsichtlich der Auswertung und Rückgabe von in Ermittlungen beschlagnahmter Informationstechnik?

Die Praxis der Bundesbehörden richtet sich nach den geltenden Gesetzen sowie der in Auslegung dieser Gesetze entwickelten Rechtsprechung.

a) Inwieweit versuchen Bundesbehörden, eine unnötige Beschlagnahme durch eine forensische Datensicherung vor Ort zu vermeiden?

Ob die Gewinnung eines – forensischen Ansprüchen genügenden – Datenträgerabbilds vor Ort möglich ist, hängt neben den vorhandenen Ressourcen insbesondere von Zustand und Eigenschaften des jeweiligen Rechnersystems ab. Über die Notwendigkeit einer Sicherstellung kann deshalb nur nach den Umständen des Einzelfalls entschieden werden. Gleiches gilt für ähnliche Maßnahmen, durch die in geeigneten Fällen Sicherstellungen vermieden werden können, wie zum Beispiel die Durchsicht von Datenträgern zur Ausscheidung erkennbar nicht beweiserheblicher Daten. Dabei kann auch – etwa wenn Zugangssicherungen wie Passwörter und Verschlüsselungen genutzt worden sind – die Kooperationsbereitschaft der Betroffenen eine erhebliche Rolle spielen.

b) Inwieweit wird durch Bundesbehörden im Falle einer Mitnahme der Technik der Verhältnismäßigkeitsgrundsatz beachtet?

Der Verhältnismäßigkeitsgrundsatz genießt Verfassungsrang und ist daher für sämtliche Ermittlungsmaßnahmen leitend.

c) Inwieweit ist es nach Kenntnis der Bundesregierung Praxis, dass die Polizei beziehungsweise die Staatsanwaltschaft die Beschlagnahme so schnell wie möglich wieder aufhebt?

Die Beschlagnahme eines Gegenstandes innerhalb eines Ermittlungsverfahrens ist aufzuheben, wenn der Beschlagnahmegrund nachträglich wegfällt, sich herausstellt, dass von vornherein kein Beschlagnahmegrund vorgelegen hat oder wenn die Maßnahme sich zwischenzeitlich als nicht mehr verhältnismäßig erweist. Der Bundesregierung liegen keine Anhaltspunkte dafür vor, dass diese rechtlichen Vorgaben von den Ermittlungsbehörden außer Acht gelassen würden. Im Übrigen können Betroffene jederzeit eine gerichtliche Entscheidung beantragen (§ 98 Absatz 2 Satz 2 der Strafprozessordnung [StPO]).

d) Welche Schlussfolgerungen zieht die Bundesregierung aus dem Urteil des Amtsgerichts Reutlingen, wonach Ermittlungsbehörden die Technik in einem Zeitraum von drei Werktagen sichern und zurückgeben müssen (Beschluss vom 5. Dezember 2011)?

Der Beschluss des Amtsgerichts Reutlingen vom 5. Dezember 2011 (5 Gs 363/11) betrifft einen Einzelfall, in dem die Beschlagnahme von Datenträgern bei einem gewerblichen Hostprovider Interessen unbeteiligter Dritter beeinträchtigt haben soll. Nach Auffassung der Bundesregierung gestattet die Entscheidung keine über diesen Einzelfall hinausgehenden Schlussfolgerungen. Insbesondere lässt sich den Entscheidungsgründen der in der Fragestellung behauptete Rechtssatz nicht entnehmen. Im Übrigen nimmt die Bundesregierung vor dem Hintergrund der verfassungsrechtlich garantierten Gewaltenteilung davon Abstand, die in

richterlicher Unabhängigkeit getroffene Entscheidung des Amtsgerichts Reutlingen zu kommentieren.

e) Inwieweit wurde im konkreten Fall der 106 Razzien durch das BKA und andere beteiligte Behörden versucht, eine unnötige Beschlagnahme durch eine forensische Datensicherung vor Ort zu vermeiden?

Auf die Antwort zu Frage 4 wird verwiesen.

6. Welche technischen Werkzeuge (Soft- und Hardware) wurden zur forensischen Auswertung der beschlagnahmten Technik genutzt?

a) Kam zur forensischen Auswertung der Mobiltelefone seitens der Bundesbehörden oder – nach Kenntnis der Bundesregierung – Landesbehörden Technik der Firmen Micro Systemation, Cellebrite, Oxygen Software GmbH, COMPELSON oder anderer in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/10077 genannten Firmen zum Einsatz?

b) Inwieweit kamen zur Auswertung und Analyse der sichergestellten Daten Anwendungen der Hersteller rola Security und IBM zum Einsatz?

Auf die Antwort zu Frage 4 wird verwiesen.

c) Welche „unterschiedliche[n] kriminalistische[n] Fragestellungen“ können mit der hier erfragten Technik überhaupt bearbeitet werden (Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/6587)?

Bei der Technik der Firmen Micro Systemation, Cellebrite, Oxygen Software GmbH und COMPELSON handelt es sich um Hard- und Softwarekomponenten zur Auswertung von Mobiltelefonen. Diese Technik ermöglicht das Auslesen, Speichern, Darstellen und Auswerten der auf Mobiltelefonen gespeicherten Daten (Adressbuch, Anruflisten usw.) für kriminalistische Fragestellungen.

Software der Fa. Rola Security dient als Fallbearbeitungssystem mit Möglichkeiten zur Beziehungsanalyse. IBMs Criminal Reduction Utilising Statistical History ist ein prediktives Analyseprogramm, mit dem Aussagen über die Örtlichkeit möglicher zukünftiger Straftaten ermöglicht werden sollen.

d) Welche „unterschiedliche[n] kriminalistische[n] Fragestellungen“ wurden mit der aufgeführten Technik im Einzelfall der hier nachgefragten GEMA-Proteste bearbeitet?

Auf die Antwort zu Frage 4 wird verwiesen.

7. Wurden Verdächtige im Zusammenhang mit Ermittlungen wegen offensichtlich politisch motivierten, massenhaften DoS-Anfragen auch mit verdeckten Ermittlungen infiltriert?

a) Haben Bundesbehörden mit Informanten/Informantinnen oder verdeckten Ermittlern/Ermittlerinnen entsprechende Zusammenhänge ausspioniert bzw. von verdeckt operierenden Beamten/Beamtinnen der Landesbehörden gelieferte Informationen verarbeitet?

b) Wurde bei den Ermittlungen Software zum Eindringen in private Rechnersysteme (Trojaner) eingesetzt?

c) Kamen in den Ermittlungen auch Maßnahmen der Funkzellenauswertung zur Anwendung?

Von Bundesbehörden wurden keine verdeckten Ermittlungsmaßnahmen durchgeführt oder Informationen von verdeckten Ermittlern/Informanten verarbeitet. Im Übrigen liegen der Bundesregierung keine über die Antworten zu den Fragen 1 und 2a hinausgehenden Erkenntnisse über die in der Zuständigkeit der betroffenen Länder geführten Verfahren vor.

8. Trifft die Aussage des Amtsgerichts Wiesbaden nach Ansicht der Bundesregierung zu, dass „obwohl eine Vielzahl von Personen dem Aufruf von ‚Anonymous' folgten, […] der Internetauftritt der GEMA zu keinem Zeitpunkt unerreichbar [war]" und stattdessen lediglich die „Datenverarbeitungsgeschwindigkeit reduziert" gewesen ist (http://politgirl.wordpress.com/2012/06/12/rechner-beschlagnahmt, 14. Juni 2012)?

   Sind nach Ansicht von Bundesbehörden in diesem Fall kommerzielle Interessen tangiert, sodass Schadenersatzansprüche geltend gemacht werden können?

Die Bundesregierung sieht insbesondere vor dem Hintergrund der verfassungsrechtlich garantierten Gewaltenteilung keine Veranlassung, zu der in richterlicher Unabhängigkeit getroffenen Entscheidung des Amtsgerichts Wiesbaden inhaltlich Stellung zu nehmen. Grundsätzlich können aus § 823 Absatz 2 des Bürgerlichen Gesetzbuches in Verbindung mit § 303b des Strafgesetzbuches (StGB) Schadensersatzansprüche infolge von DDoS-Attacken bestehen. Ob allein die Reduzierung der Datenverarbeitungsgeschwindigkeit zu einem kompensationsfähigen Schaden führen kann, ist eine Frage des Einzelfalles.

9. Trifft es nach Kenntnis der Bundesregierung zu, dass die GEMA Daten weiterer Proteste an Bundes- oder Landesbehörden übergeben hat (Meldung der dapd, Onlineausgabe MZ, 15. Juni 2012)?

   a) Falls ja, um welche Aktionen und Daten handelte sich?

   b) Inwieweit hat die GEMA zur Verfolgung der Proteste im Dezember 2011 und Juni 2012 (oder etwaiger anderer) selbst eine Strafanzeige gestellt?

Mit Ausnahme der Strafanzeige, die den Ermittlungen des BKA zu Grunde lag, sind der Bundesregierung keine weiteren Strafanzeigen bekannt, die Ermittlungsbehörden in ihrem Zuständigkeitsbereich betreffen.

10. Wie bewertet die Bundesregierung die Strafbarkeit einer Nutzung von Werkzeugen wie LOIC?

   a) Wie bewertet die Bundesregierung die Strafbarkeit eines Besitzes von Werkzeugen wie LOIC?

   b) Wie bewertet die Bundesregierung die Strafbarkeit einer Herstellung von Werkzeugen wie LOIC?

   c) Trifft die Bewertung von Werkzeugen wie LOIC auch auf Add ons für handelsübliche Browser zu, die ebenfalls massenhafte Besuchsanfragen für eingestellte Webseiten bewerkstelligen können?

Die Frage, ob bestimmte Computerprogramme („Werkzeuge") von strafrechtlichen Bestimmungen erfasst werden, ist im Einzelfall von den Strafverfolgungsbehörden und den Gerichten zu beurteilen. Die Bundesregierung kann insoweit zu einzelnen Computerprogrammen keine Stellungnahme abgeben.

Unabhängig von dem konkreten Fall kann darauf hingewiesen werden, dass bei einer Nutzung von Computerprogrammen zur Herbeiführung einer „Denial of

Service-Attacke“ eine Strafbarkeit wegen Computersabotage nach § 303b StGB in Betracht kommen kann. Bei einer solchen Attacke werden die Dienste eines Servers durch eine Vielzahl von Anfragen derart belastet, dass dessen Aufnahme- und Verarbeitungskapazität nicht ausreicht und somit der Zugang für berechtigte Kontaktaufnahmen mit dem Server blockiert oder zumindest erschwert wird. Bei einem koordinierten Angriff, der von einer größeren Anzahl anderer Systeme ausgeht, wird von einer „verteilten Dienstblockade“ gesprochen (DDoS-Attacke).

Nach § 303b Absatz 5 in Verbindung mit § 202c Absatz 1 Nummer 2 StGB kann sich darüber hinaus strafbar machen, wer Computerprogramme, deren Zweck die Begehung einer Computersabotage ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Eine Strafbarkeit wegen des Besitzes solcher Programme ist nicht vorgesehen. Zudem ist zu berücksichtigen, dass das Programm mit der Absicht entwickelt oder modifiziert worden sein muss, es zur Begehung einer Straftat der Computersabotage einzusetzen. Diese Absicht muss sich auch objektiv manifestiert haben. Nicht ausreichend ist, dass ein Programm – wie das für sogenannte dual use tools gilt – für die Begehung von Computerstraftaten lediglich geeignet oder auch besonders geeignet ist (siehe BVerfG, 2 BvR 2233/07 vom 18. Mai 2009, Rn. 61).

11. Inwieweit verfolgen Bundesbehörden in dem Ermittlungsverfahren zu den Protesten bei der GEMA, ob Werkzeuge wie LOIC oder andere (auch Add ons) heruntergeladen wurden?

    Auf welche Weise arbeiten Ermittler hierzu mit Telekommunikationsprovidern zusammen?

Das BKA verfolgte in dem Ermittlungsverfahren nicht, ob die genannten Werkzeuge heruntergeladen wurden. Ob diese durch die Beschuldigten genutzt wurden, ist letztlich nur durch eine Auswertung der Beweismittel möglich. Hierzu wird auf die Antwort zu Frage 4 verwiesen.

12. Inwieweit sind Bundesbehörden mit weiteren Ermittlungen gegen vermeintliche „Anonymous“-Aktivisten befasst?

Die Bundesregierung nimmt zu laufenden Ermittlungsverfahren nicht Stellung, sofern dadurch deren Erfolg gefährdet würde. Davon umfasst ist auch die Beantwortung der Frage, ob überhaupt Ermittlungsverfahren eingeleitet worden sind, da bereits das Bekanntwerden eines laufenden Ermittlungsverfahrens geeignet ist, dessen Erfolg zu gefährden. Die Bundesregierung orientiert sich dabei an der Rechtsprechung des Bundesverfassungsgerichts, wonach aus Artikel 38 Absatz 1 Satz 2 und Artikel 20 Absatz 2 Satz 2 des Grundgesetzes (GG) ein Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung folgt, an dem die einzelnen Abgeordneten und die Fraktionen teilhaben und dem grundsätzlich eine Antwortpflicht der Bundesregierung korrespondiert (vgl. BVerfGE 124, 161, 188). Die Antwortpflicht der Bundesregierung unterliegt indes verfassungsrechtlichen Grenzen. Die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind die wesentlichen Aufgaben der Strafrechtspflege, die zum Schutz der Bürger den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen soll. Strafnormen und deren Anwendung in einem rechtsstaatlichen Verfahren sind Verfassungsaufgaben (BVerfGE 107, 104, 118 f.). Nach Abwägung des parlamentarischen Fragerechts mit dem verfassungsrechtlichen Gebot, eine funktionsfähige Strafjustiz zu gewährleisten, kön-

nen wegen der ansonsten bestehenden Gefährdung des Erfolgs von Ermittlungsverfahren hier keine näheren Angaben zu deren etwaiger Einleitung gemacht werden.

a) Welche Abteilungen welcher Behörden sind hieran beteiligt?

b) Welche Arbeitsgruppen oder sonstigen Strukturen existieren hierfür?

c) Inwieweit werden die Ermittlungen mit den Bundesländern abgestimmt?

Auf die Antwort zu Frage 12 wird verwiesen.

d) Welche Datensammlungen wurden zu Aktionen von „Anonymous“ oder ähnlichen Gruppierungen bzw. Netzwerken angelegt?

Seitens Bundesbehörden wurden bisher keine expliziten Datensammlungen zu Aktionen von Anonymous angelegt. Gleichwohl fallen im Rahmen der gesetzlichen Aufträge der Sicherheitsbehörden Informationen zu internationalen Hackergruppierungen an.

Im Rahmen von Ermittlungen, wie im vorliegenden Fall, erfolgt eine Datenerfassung für den jeweiligen Einzelfall in den polizeilichen Informationssystemen bzw. den polizeilichen Datensammlungen.

13. Inwieweit arbeiten die Behörden in Ermittlungen gegen vermeintliche „Anonymous“-Aktivisten auch mit internationalen Institutionen zusammen?

Das BKA nimmt im Rahmen seiner Aufgaben gemäß § 3 BKAG die Rolle des Nationalen Zentralbüros für Interpol wahr und ist nationale Stelle für Europol. Gemäß § 3 Absatz 2 Satz 1 BKAG umfasst dies den zur Verhütung oder Verfolgung von Straftaten erforderlichen Dienstverkehr der Polizeien des Bundes und der Länder mit den Polizei- und Justizbehörden sowie sonstigen insoweit zuständigen öffentlichen Stellen anderer Staaten. Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

a) Inwieweit werden Ermittlungen auch mit der EU-Polizeiagentur Europol und mit Interpol geführt?

Auf die Antwort zu Frage 13 wird verwiesen.

b) An welchen Treffen hierzu haben welche Stellen des Bundesministeriums des Innern in den letzten zwei Jahren teilgenommen?

Das Bundesministerium des Innern hat an derartigen Treffen nicht teilgenommen.

c) Inwieweit sind Bundesbehörden mit Ermittlungen gegen den Filehoster PirateBay befasst?

Auf die Antwort zu Frage 12 wird verwiesen.

14. Inwieweit waren Bundesbehörden in die „Operation Unmask“, die im Februar 2012 von Interpol mittels Razzien in verschiedenen Ländern gegen vermeintliche „Anonymous“-Aktivisten ausgeführt wurde, informiert oder haben etwa durch Bereitstellung von „Erkenntnissen“ oder anderen Kapazitäten sogar daran teilgenommen (Guardian, 29. Februar 2012)?

Bundesbehörden waren zu keinem Zeitpunkt in die „Operation Unmask“ eingebunden. Das BKA wurde über diese Operation nach Abschluss informiert.

a) Was war das Ziel der „Operation Unmask“?

Die Operation Unmask war eine gemeinsame Operation der Länder Argentinien, Kolumbien, Chile und Spanien unter der Koordinierung von INTERPOLs Latin American Working Group of Experts on Information Technology Crime. Ziel der Operation war die Enttarnung und Ermittlung von zahlreichen Tatverdächtigen, die im Verdacht stehen Angehörige der Anonymous Gruppierung zu sein und in dieser Rolle zahlreiche Hacking Attacken gegen Privatpersonen und andere Institutionen durchgeführt zu haben. Bis zum Februar 2012 wurden 25 Personen festgenommen und zahlreiche Beweismittel sichergestellt.

b) In welchen internationalen Arbeitsgruppen wurde die „Operation Unmask“ vor oder nach den Razzien erörtert?

Diese Operation wurde dem BKA im Mai 2012 durch das Generalsekretariat von INTERPOL im Rahmen der allgemeinen Berichterstattung während eines Arbeitsgruppentreffens der „INTERPOL European Group of Experts on Information Technology Crime“ im Nachgang vorgestellt. Ermittlungsdetails wurden nicht ausgetauscht.

c) Auf welche Art und Weise waren kommerzielle, private Unternehmen in die Ermittlungen, Razzien oder Auswertung der „Operation Unmask“ eingebunden?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

15. Inwieweit waren Bundesbehörden in die „Operation Thunder“ eingebunden, die gleichzeitig zur „Operation Unmask“ von Europol ausgeführt wurde und dort als erfolgreicher Schlag gegen „eine Gruppe von Hackern“ gewertet wird (Pressemitteilung, 28. Februar 2012)?

Bundesbehörden waren zu keinem Zeitpunkt in die Operation eingebunden.

Auch diese Operation wurde dem BKA im Mai 2012 durch das Generalsekretariat von INTERPOL im Rahmen der allgemeinen Berichterstattung während eines Arbeitsgruppentreffens der „INTERPOL European Group of Experts on Information Technology Crime“ im Nachgang vorgestellt. Ermittlungsdetails wurden nicht ausgetauscht.

a) Welche Handlungen sollen die Verdächtigen vorgenommen haben?

b) Inwieweit hat sich die leitende Spanish National Police Cyber Crime Unit (BIT) in den Ermittlungen an Bundesbehörden gewandt?

c) Auf welche Weise hatte Europol die „Operation Unmask“ mit der „Operation Thunder“ abgestimmt?

d) Auf welche Art und Weise waren kommerzielle, private Unternehmen in die Ermittlungen, Razzien oder Auswertung der „Operation Thunder“ eingebunden?

Der Bundesregierung liegen diesbezüglich keine Erkenntnisse vor. Die „Spanish National Police Cyber Crime Unit“ (BIT) hat sich bei den in Rede stehenden Ermittlungen nicht an Bundesbehörden gewandt.

16. Auf welche Art und Weise war das Europol Cyber Crime Centre in die „Operation Unmask“ und „Operation Thunder“ eingebunden?

Die Einrichtung des „Europol Cyber Crime Centre“ ist noch nicht erfolgt. Insofern kann dieses auch nicht in die benannten Operationen eingebunden worden sein.

a) Wurden in diesem Zusammenhang von Europol aus den EU-Mitgliedstaaten gelieferte Vorratsdaten ausgewertet?

Der Bundesregierung liegen diesbezüglich keine Erkenntnisse vor.

b) In welchen Datensammlungen werden bei Europol Aktivitäten von „Anonymous“ oder ähnlichen Protestformen abgelegt?

Der Bundesregierung liegen diesbezüglich keine Erkenntnisse vor.

c) Inwieweit werden politische Internetproteste, wie etwa die gemeinsamen Besuche der GEMA-Website, bei Europol in der Analysearbeitsdatei „Cyborg“ gespeichert?

Eine Speicherung in der Analysearbeitsdatei „Cyborg“ erfolgte mangels internationaler Bezüge nicht. Sofern DDoS-Attacken eine internationale Dimension und die rechtlichen Einstellungsvoraussetzungen aufweisen, basiert die Einstellung in die Analysearbeitsdatei „Cyborg“ auf der Prüfung im Einzelfall.

17. Nach welcher Maßgabe wird von Bundesbehörden bestimmt, ob ein Besucher eine Website lediglich blockiert, eine Datenveränderung vornimmt oder ob es sich um eine Computersabotage handelt?

Ob eine DDoS-Attacke eine Straftat im Sinne des § 303b StGB (Computersabotage) darstellt, obliegt der Prüfung im Einzelfall durch die zuständigen Strafverfolgungsbehörden und Gerichte. Allgemeine Vorschriften zur Einschätzung gibt es bei Bundesbehörden nicht.

a) Welche technischen Werkzeuge stehen zur Bestimmung der Angriffstiefe zur Verfügung?

Generell stehen alle technischen Werkzeuge zur Netzwerkanalyse zur Verfügung.

b) An welchen Richtlinien orientieren sich Bundesbehörden bei der Klassifizierung derartiger Angriffe oder massenhafter Besuche?

Auf die Antwort zu Frage 17 wird verwiesen.

18. Inwieweit teilt die Bundesregierung die Ansicht der Fragesteller/Fragestellerinnen, dass die gemeinsamen, gleichzeitigen Besuche der GEMA-Website als politischer Protest zu werten sind, zumal dies unter anderem unter dem Motto „GEMA nach Hause“ auch im Internet veröffentlicht wurde (z. B. www.youtube.com/watch?v=ibN28v-VLr4)?

a) Teilt die Bundesregierung die Meinung, dass die Handlungen der im Rahmen der GEMA-Proteste mit Repressionen bedachten Jugendlichen im Internet eher als virtuelle Sitzblockade zu betrachten sind, als als versuchte Computersabotage?

b) Inwieweit teilt die Bundesregierung die Einschätzung der Fragesteller/Fragestellerinnen, dass es bei der juristischen und politischen Beurteilung der Handlungen darauf ankommt, ob die gemeinsame Aktion oder aber der möglich angerichtete Schaden im Mittelpunkt stand?

c) Inwieweit teilt die Bundesregierung die Einschätzung der Fragesteller/Fragestellerinnen, dass es sich bei den Protesten nicht um Sachbeschädigung handeln kann, sondern allenfalls um eine „Unterdrückung" eines Datenstroms?

19. Besteht nach Ansicht der Bundesregierung ein Bedarf für die Regelung eines virtuellen Demonstrationsrechts?

a) Sieht die Bundesregierung einen rechtlichen Spielraum, der es erlauben würde, Aktionen, die darauf gerichtet sind, die Erreichbarkeit von Webseiten durch massenhafte Nutzeranfragen zu behindern, als Protestaktionen, virtuelle Demonstrationen oder virtuelle Sitzblockaden einzuordnen?

b) Inwieweit haben Bundesbehörden juristisch geprüft, ob sich Initiatoren von Onlinedemonstrationen auf das Demonstrationsrecht berufen können, wie es eine Sprecherin des Bundesministeriums der Justiz 2001 gegenüber heise.de andeutete (www.heise.de/tp/artikel/7/7907/1.html)?

Die Beurteilung des konkreten Vorgangs obliegt den Strafverfolgungsbehörden und Gerichten.

Unabhängig von dem konkreten Fall kann darauf hingewiesen werden, dass es für eine Strafbarkeit wegen Computersabotage nach § 303b Absatz 1 Nummer 1 StGB darauf ankommt, dass der Täter in der Absicht handelt, einem anderen einen Nachteil zuzufügen. Dazu muss der Täter mit dem Bewusstsein vorgehen, dass eine nachteilige Folge oder Beeinträchtigung rechtmäßiger Interessen die notwendige Folge seiner Tat ist. Der Rechtsausschuss des Deutschen Bundestages hat hierzu in seinem Bericht vom 23. Mai 2007 zu der entsprechenden Gesetzesänderung ausgeführt, dass er davon ausgehe, dass sogenannte Massen-E-Mail-Proteste ohne eine solche Nachteilszufügungsabsicht geschähen und nicht den Tatbestand der Computersabotage erfüllten, sondern von der Meinungsfreiheit nach Artikel 5 GG gedeckt seien (Bundestagsdrucksache 16/5449, S. 5, vom 12. April 2011). Damit besteht aus Sicht der Bundesregierung bereits auf der Basis des geltenden Rechts ausreichend Spielraum für die Strafverfolgungsbehörden und Gerichte, um bei politisch motivierten Protestaktionen Aspekte der Meinungsfreiheit erforderlichenfalls zu berücksichtigen.

Was die Frage des Versammlungsrechts angeht, so ist darauf hinzuweisen, dass eine Versammlung im Sinne von Artikel 8 des Grundgesetzes die gleichzeitige körperliche Anwesenheit mehrerer Personen an einem Ort erfordert. Mangels Körperlichkeit sind virtuelle Versammlungen etwa im Internet daher im verfassungsrechtlichen Sinne keine „Versammlungen". Aus dem angesprochenen Artikel (www.Heise.de/tp/artikel/7/7907/1.html) ergibt sich keine andere Bewertung.

20. Wie beurteilt die Bundesregierung die Sinnhaftigkeit von Websperren, wie sie etwa YouTube für nicht von der GEMA freigegebene Inhalte den jeweiligen Besuchern/Besucherinnen vorzeigt?

Welche Dienste, Add ons oder andere Werkzeuge sind Bundesbehörden bekannt, mit denen sich die Sperren mühelos umgehen lassen?

Soweit youtube sein Angebot länderspezifisch ausrichtet, ist dies eine unternehmerische Entscheidung. Die Bundesregierung sieht keine Veranlassung, die Sinnhaftigkeit unternehmerischer Entscheidungen zu kommentieren.

Es ist allgemein bekannt, dass für bestimmte Formen von Websperren Umgehungsmöglichkeiten bestehen. Die Komplexität der Verfahren, mit denen Websperren umgangen werden können, differiert je nach konkreten Details des jeweiligen Sperrverfahrens. Der Bundesregierung ist das von youtube eingesetzte Sperrverfahren nicht näher bekannt, so dass eine Beurteilung der Umgehungsmöglichkeiten nicht erfolgen kann.

21. Trifft es nach Kenntnis der Bundesregierung zu, dass die ermittelnde Staatsanwaltschaft die Repression öffentlich als „heilsame Schockwirkung“ bezeichnet hat?

Der Bundesregierung liegen über die bereits in der Vorbemerkung dieser Kleinen Anfrage angeführten Presseveröffentlichung hinaus keine weiteren Erkenntnisse vor. Im Übrigen sieht die Bundesregierung keine Veranlassung, die Einschätzung der Justizorgane zu kommentieren.

a) Falls ja, worin besteht diese nach Ansicht der Bundesregierung?

Auf die Antwort zu Frage 21 wird verwiesen.

b) Haben Bundesbehörden im Rahmen der Ermittlungen wegen der GEMA-Proteste nach Kenntnis des entsprechenden Programms bei PasteHTML jemals dessen Löschung ersucht?

Bundesbehörden haben nicht um Löschung ersucht.

c) Falls nein, warum nicht?

Gefahrenabwehrmaßnahmen, wie das Ersuchen um Löschung von Webseiten, fallen grundsätzlich in die Zuständigkeit der Landesbehörden soweit sie nicht Bundesbehörden zugewiesen sind.

22. Ist den ermittelnden Behörden bekannt, ob der Link bei PasteHTML inzwischen gelöscht ist?

Falls ja, von wem wurde die Löschung veranlasst?

Nach Kenntnis des BKA ist der für die DDoS-Attacken auf die GEMA-Webseiten genutzte Link bei pastehtml.com über eine standardmäßig genutzte IP-Adresse mit Stand 17. Juli 2012 weiterhin erreichbar.

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