Deutscher Bundestag **Drucksache 17/11969**

17. Wahlperiode 20. 12. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Herbert Behrens, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/11757 –

Zusammenarbeit deutscher Behörden bei „grenzüberschreitenden europäischen Cybersicherheitsvorfällen“

Vorbemerkung der Fragesteller

Zur „Bekämpfung der Cyberkriminalität und zum Verbraucherschutz beim elektronischen Geschäftsverkehr“ will die Europäische Union ab Januar 2013 ein eigenes „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ errichten. Laut einem Vorschlag soll es im Europäischen Polizeiamt Europol in Den Haag angesiedelt werden. Das Zentrum soll als „europäische Schaltstelle für die Bekämpfung von Cyberstraftaten“ dienen. Dabei geht es nicht nur um Strafverfolgung, sondern auch um „Gefahrenabwehr“: „Cyberstraftaten bei elektronischen Bankgeschäften und Onlinebuchungen“ soll vorgebeugt werden. Die Zuständigkeitsbereiche sind aber unklar, zumal über das Internet begangene Straftaten gegen die sexuelle Selbstbestimmung oder „Cyberangriffe“ auf Infrastrukturen und Informationssysteme in der EU bereits jetzt von Europol verfolgt werden. Im September 2012 hat die Europäische Union zudem ihr zunächst provisorisches „Computer Emergency Response Team“ (CERT-EU) in eine permanente Einrichtung überführt (heise.de, 12. September 2012). Das CERT-EU ist für die Sicherheit aller Netze von EU-Institutionen, einschließlich des Europäischen Gerichtshofs und der Europäischen Zentralbank zuständig.

Bezüglich „Cyberkriminalität“ geht es nach Ansicht der Fragesteller um die Inszenierung einer neuen Gefahr, die dann zur Ergreifung weiterer Maßnahmen ins Feld geführt wird. So erklärt auch die Europäische Kommissarin für Inneres, Cecilia Malmström: „Wir dürfen nicht zulassen, dass Cyberkriminelle unser digitales Leben zerrütten“ (Pressemitteilung der Europäischen Kommission, 28. März 2012). Cecilia Malmström will die „Freiheit, die Offenheit und die Sicherheit des Internets“ gewahrt wissen. Indes betreiben die Europäische Kommission und der EU-Anti-Terrorbeauftragte auf mehreren Ebenen eine Einschränkung des Internets und des Datenschutzes. Mit der Begründung der Abwehr von „Cyberterrorismus“ werden zahlreiche Maßnahmen vorgeschlagen, obschon es bis heute keinen bekannten „cyberterroristischen“ Vorfall gegeben hat. Dies bestätigt die Bundesregierung (Bundestagsdrucksache 17/7578).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 17. Dezember 2012 übermittelt.

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

Deshalb steht zu vermuten, dass das „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ lediglich die Arbeit von Europol festschreiben soll. So spricht auch die Kommission in ihrer Pressemitteilung davon, die Polizeiagentur solle im Rahmen des „EU-Zentrums zur Bekämpfung der Cyberkriminalität“ die Mitgliedstaaten „durch computerforensische Hilfe oder durch Mitwirkung bei der Zusammenstellung gemeinsamer Untersuchungsteams“ operativ unterstützen. Hierfür soll Europol „Informationen aus offenen Quellen, aus der Privatwirtschaft, von Polizeidiensten und aus akademischen Kreisen zusammentragen“. Umgekehrt sollen entsprechende Anfragen von „Ermittlern, Richtern und Staatsanwälten sowie aus dem Privatsektor“ beantwortet werden. Neben der Informationsbeschaffung soll Europol insbesondere mit „privatwirtschaftlichen Unternehmen“ zusammenarbeiten. Die Unvoreingenommenheit des „EU-Zentrums zur Bekämpfung der Cyberkriminalität“ kann also bezweifelt werden. Hinzu kommt, dass die Einrichtung des Zentrums womöglich den Prinzipien der Europäischen Union zuwiderläuft: Einrichtungen der EU dürfen keine Aufgaben übernehmen, die bereits in den Mitgliedstaaten verrichtet werden.

1. Auf welche Weise soll das „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ in den operativen Betrieb übergehen?

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität soll der Abteilung „Operations Department“ von Europol zugeordnet werden und im Januar 2013 seine Arbeit aufnehmen. Eigene Ermittlungen bzw. operative Tätigkeiten des Zentrums, das seine Aufgaben zunächst auf der Grundlage des geltenden EUROPOL-Verordnung wahrnehmen soll, sind nicht vorgesehen.

a) Welche Aufgabe hat das Zentrum, und wie korrespondiert es mit Strukturen der Bundesregierung, die sich ebenfalls mit „Cybersicherheit“ befassen?

Vorbehaltlich der Budget- und Haushaltsplanung sind derzeit folgende vier Aufgabenbereiche für das Europäische Zentrum zur Bekämpfung der Cyberkriminalität vorgesehen:

1. Data fusion function
   „Wissenszentrum für die Mitgliedstaaten“, z.B. Sammlung und Aufbereitung von Cybercrime-relevanten Daten sowie Koordinierung von Anfragen und Auswertungen.
2. The Operation function
   Unterstützung für die operativen Arbeit der Mitgliedstaaten in technischer, analytischer und forensischer Hinsicht.
3. R&D and training function
   Ausbildung, Forschung und Awareness-Initiativen, Aufbau eines Experten-Netzwerks.
4. Strategy function
   Bearbeitung von strategischen Angelegenheiten und Auswertung operativer Entwicklungen.

b) Wo wird das Zentrum angesiedelt, und mit welchen Mitarbeiterinnen und Mitarbeitern wird es nach derzeitiger Planung ausgestattet?

Nach derzeitigem Kenntnisstand der Bundesregierung wird der Personalbedarf durch Mitarbeiter von Europol gedeckt.

c) Wie viele der Mitarbeiterinnen und Mitarbeiter gehören zu welchen Abteilungen der Polizeiagentur Europol?

Derzeit sind bei Europol ca. 700 Mitarbeiter beschäftigt. Wie sich diese auf die einzelnen Abteilungen aufteilen, ist der Bundesregierung nicht bekannt.

d) Inwieweit und mit welchen Kapazitäten sind Behörden aus „Drittstaaten“ eingebunden?

Nach Kenntnis der Bundesregierung sind Drittstaaten nicht in die Arbeit des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität eingebunden.

Soweit Europol mit einem Drittstaat ein Abkommen abgeschlossen hat, das Regelungen über die operative Zusammenarbeit enthält, kann der Drittstaat auf dieser Grundlage an der operativen Kriminalitätsauswertung im Europäischen Zentrum zur Bekämpfung der Cyberkriminalität teilnehmen.

e) Welche internationalen Organisationen, Internetdienstleister oder Interessenverbände sind am „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ beteiligt?

Nach Kenntnis der Bundesregierung sind keine sonstigen Organisationen an dem Zentrum beteiligt. Allerdings sind strategische Partnerschaften mit dem Privatsektor langfristig beabsichtigt.

f) Welche Firmen oder Banken sollen weshalb am „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ beteiligt werden?

g) Inwieweit und auf welche Art und Weise werden die nationalen „Computer Emergency Response Teams“ in das „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ eingebunden?

Auf die Antwort zu Frage 1e wird verwiesen.

2. Inwieweit und auf welche Art und Weise soll das „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ die bereits existierenden analytischen und forensischen Kapazitäten Europols unterstützen (Europol Work Programme 2013, Ratsdokument 12667/12)?

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität soll in erster Linie im Rahmen der geltenden Rechtsgrundlagen die operative Tätigkeit der Mitgliedstaaten analytisch und forensisch unterstützen.

a) Auf welche Art und Weise sollen diesbezüglich Europols „intelligence analysis tools“ ausgebaut oder ersetzt werden?

b) Worum geht es bei der „EAS Evolution initiative“ von Europol?

d) Was ist damit gemeint, wenn Europol neue „means of modern information processing tools“ entwickelt (Europol Work Programme 2013, Ratsdokument 12667/12)?

Dazu liegen der Bundesregierung keine Informationen vor.

c) Wie ist die Bundesregierung daran beteiligt?

Die Bundesregierung ist daran nicht beteiligt.

3. Inwieweit ist das CERT-EU von einem Pilotprojekt zu einer permanenten Einrichtung geworden (heise.de, 12. September 2012)?

Das CERT-EU wurde nach einer einjährigen Pilotphase mit anschließender Evaluierung in eine permanente Einrichtung überführt. Zugrunde liegt ein interinstitutioneller Beschluss der Generalsekretariate der EU-Institutionen vom 9. August 2012. Die Europäische Kommission hat daraufhin am 11. September 2012 die dafür notwendigen administrativen Maßnahmen veranlasst. Die Mittel für CERT-EU werden von den großen Institutionen und Agenturen der EU bereitgestellt, u. a. von der Kommission, dem Rat, dem Europäischen Parlament, dem Ausschuss der Regionen, dem Europäischen Wirtschafts- und Sozialausschuss und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA).

a) Mit welcher Aufgabenstellung wurde das CERT-EU errichtet?

In der Digitalen Agenda für Europa, die im Mai 2010 beschlossen wurde, verpflichtete sich die Kommission, im Rahmen des allgemeinen Engagements für eine verstärkte und auf hoher Ebene getragenen Politik für die Netz- und Informationssicherheit in Europa ein CERT für die EU-Institutionen aufzubauen. Im Juni 2011 wurde unter der Federführung der Vizepräsidenten der Kommission, Neelie Kroes und Maroš Šefčovič, das CERT-EU als zunächst einjähriges Pilotprojekt eingerichtet (CERT-EU pre-configuration team). Das CERT-EU wurde mit der Zielsetzung errichtet, die EU-Institutionen, EU-Organe und EU-Agenturen beim Schutz ihrer IT-Systeme und -Infrastrukturen vor Cyber-Angriffen und Störungen zu unterstützen. Dazu bietet ihnen das CERT-EU Dienstleistungen an, die präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in IT-Systemen umfassen. Dazu gehören die Warnung vor Schwachstellen in Hardware- und Softwareprodukten, Handlungsempfehlungen zur Schadensvermeidung und Schadensbegrenzung oder -beseitigung sowie die Unterstützung bei der Reaktion auf eintretende IT-Sicherheitsvorfälle. Zu diesem Zweck soll das CERT-EU eng mit den jeweiligen IT-Sicherheitsteams der einzelnen EU-Institutionen zusammenarbeiten.

b) Über wie viele Mitarbeiterinnen und Mitarbeiter verfügt das CERT-EU, und wo ist es angesiedelt?

Das Team des CERT-EU setzt sich aus elf Mitarbeitern (Stand: 14. September 2012) zusammen, die von der Europäischen Kommission, dem Generalsekretariat des Rates, dem Europäischen Parlament, den Gemeinsamen Diensten des Europäischen Wirtschafts- und Sozialausschusses und des Ausschusses der Regionen und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zur Verfügung gestellt werden. Das CERT-EU ist funktional dem Generaldirektor der Generaldirektion Informatik (DIGIT) der Europäischen Kommission unterstellt und arbeitet unter der strategischen Aufsicht eines interinstitutionellen Lenkungsausschusses.

c) Inwieweit ist das CERT-EU auch mit der Vorbeugung oder Bekämpfung speziell politisch motivierter Proteste von Gruppen wie „Anonymous“ befasst?

Das CERT-EU agiert nach Kenntnis der Bundesregierung unabhängig von möglichen Motivationen spezieller Täter bzw. Angriffsgruppen koordinierend bei der Abwehr konkreter IT-Sicherheitsvorfälle.

4. Auf welche Weise sind Regierungen von EU-Mitgliedstaaten im CERT-EU vertreten?

Das CERT-EU bietet technische CERT-Dienstleistungen für EU-Institutionen. Regierungen von EU-Mitgliedstaaten sind dort grundsätzlich nicht vertreten. In Einzelfällen können aus den Mitgliedsländern abgeordnete technische Experten als „Seconded National Experts“ die Arbeit des CERT-EU über einen begrenzten Zeitraum unterstützen.

a) Welche weiteren CERTs oder entsprechende „IT-Expertengruppen“ sind mit welchen Mitgliedern auf EU-Ebene geplant?

b) Wo wären diese angebunden, bzw. wem gegenüber wären diese rechenschaftspflichtig?

Der Bundesregierung sind derzeit keine entsprechende Planungen bekannt.

c) Auf welche Weise werden welche Institutionen der USA angebunden bzw. eingebunden, und welchen Zugriff auf Informationssysteme wird ihnen gewährt?

d) Auf welche Weise werden welche Institutionen weiterer „Drittstaaten“ angebunden bzw. eingebunden, und welchen Zugriff auf Informationssysteme wird ihnen gewährt?

Institutionen aus den USA sowie aus Drittstaaten sind nicht im CERT-EU eingebunden, und es wird ihnen nach Kenntnis der Bundesregierung auch kein Zugriff auf Informationssysteme gewährt. Es wird davon ausgegangen, dass CERT-EU im Rahmen der normalen CERT-Arbeit auch mit internationalen Institutionen zusammenarbeiten wird.

5. Auf welche Weise hat die Bundesregierung zur Entwicklung einer „umfassenden Strategie für Cyber-Sicherheit“ beigetragen, die von der Europäischen Kommission noch im Jahr 2012 vorgestellt werden soll?

a) Welche Beiträge haben Bundesbehörden hierfür erbracht?

Das Vorhaben wurde erstmalig mit dem Arbeitsprogramm der Europäischen Kommission für das Jahr 2012 vorgestellt, die Veröffentlichung in Form einer Mitteilung ist für Ende Januar 2013 vorgesehen. Der Bundesminister des Innern hatte im März 2012 ein Positionspapier an die Vizepräsidentin der Europäischen Kommission, Neelie Kroes, mit Kernforderungen übersandt. Im Juli 2012 hat die Bundesregierung zudem an einer gemeinsamen Stellungnahme „For a comprehensive European Union approach on cyberspace“ für den Europäischen Auswärtigen Dienst zusammen mit Großbritannien, Frankreich, den Niederlanden und Schweden mitgewirkt. Die Europäische Kommission hat zwischenzeitlich angekündigt, sich auf eine Strategie für Cybersicherheit zu beschränken. Weiterhin hat sich die Bundesregierung in Konsultationen aktiv eingebracht: Dies gilt insbesondere für die wiederholte Befassung mit dem Thema im European Forum for Member States (EFMS), aber auch für die Cyber Security Strategy Conference am 6. Juli 2012 in Brüssel.

b) Welche besonderen Bedrohungen haben Bundesbehörden hierfür analysiert, und was wurde der Europäischen Kommission dazu mitgeteilt?

Aus Sicht der Bundesregierung bedarf es keiner gesonderten Bedrohungslage für strategische Bündelungsmaßnahmen auf EU-Ebene zu Cybersicherheit. Staat, Wirtschaft und Gesellschaft sind in hohem Maße angewiesen auf eine sichere IT-Infrastruktur, weil Prozesse in all diesen Bereichen zunehmend über

das Internet gesteuert werden. Dieser Umstand zusammen mit den bekannten Bedrohungsszenarien (siehe Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik – BSI: „Die Lage der IT-Sicherheit in Deutschland“, 2011) zeigt bereits die Notwendigkeit auf.

6. Welche „Angriffe“ auf Computer bzw. Computersysteme von Angehörigen des Rates der Europäischen Union wurden in den Jahren 2011 und 2012 jeweils verzeichnet?

Der Bundesregierung ist die konkrete Anzahl der Angriffe auf Systeme des Rats der Europäischen Union nicht bekannt.

a) Welche Werkzeuge oder andere Mittel wurden für die „Angriffe“ verwendet?

b) Welche Urheberschaft wird für die Störungen vermutet (bitte, soweit möglich, in konkreten Zahlen angeben)?

c) Inwiefern sind davon auch die Europäische Kommission bzw. hohe Beamte der Bereiche Wirtschaft, Sicherheit und Außenpolitik betroffen?

Der Bundesregierung liegen hierzu keine Informationen vor.

7. Welche „Angriffe“ auf Computer bzw. Computersysteme von Institutionen der Bundesregierung wurden in den Jahren 2011 und 2012 jeweils verzeichnet?

Gezielte Angriffe auf Computersysteme der Bundesregierung finden durch E-Mails mit schadhaften Anhängen und durch den Download von Schadsoftware (sowohl Drive-By-Downloads als auch manuell ausgeführt) mittels HTTP statt.

a) Welche Werkzeuge oder andere Mittel wurden für die „Angriffe“ verwendet?

In der Regel werden Schadprogramme (Trojanische Pferde, Viren, etc.) für die Angriffe verwendet.

b) Welche Urheberschaft wird für die Störungen vermutet (bitte, soweit möglich, in konkreten Zahlen angeben)?

Elektronische Angriffe stellen ein effektives und nur schwer aufzuklärendes Mittel zur Informationsbeschaffung dar, bei dem insbesondere die sich bietende Anonymität des Internets eine Identifizierung der Täter extrem erschwert. Aufgrund bestimmter Merkmale und Indizien bei den erkannten Angriffen ist allerdings meist eine regionale Zuordnung der Herkunft elektronischer Angriffe möglich. Danach besitzt die überwiegende Zahl der in Deutschland festgestellten elektronischen Angriffe mit einem mutmaßlich nachrichtendienstlichen Hintergrund einen möglichen chinesischen Ursprung. Weiterhin ist davon auszugehen, dass auch andere Staaten elektronische Angriffe als Mittel zur Informationsbeschaffung nutzen.

8. Worin besteht der „freiwillige Mechanismus zur Zusammenarbeit bei grenzüberschreitenden europäischen Cybersicherheitsvorfällen“, der laut

Bundesregierung zur „Verbesserung der vorfallbezogenen europäischen Kommunikation“ erstellt wird (Bundestagsdrucksache 17/7578)?

Zur „Verbesserung der vorfallbezogenen europäischen Kommunikation“ wurde ein unverbindliches Regelwerk erstellt. Es dient dazu, im Krisenfall den Informationsaustausch und die Zusammenarbeit der Mitgliedstaaten während einer IT-Krise zu verbessern und so die gemeinsame Krisenbewältigung zu unterstützen. Das Regelwerk enthält Vorgehensweisen und Verhaltensregeln, die die Zusammenarbeit verbessern sollen.

a) Auf welche Weise wurde dieser bzw. ein vergleichbarer „Mechanismus“ entwickelt, und wer war daran beteiligt?

Der Mechanismus wurde in einer Arbeitsgruppe entwickelt, in der die nationalen Fachbehörden der EU-Mitgliedstaaten und ENISA vertreten waren.

b) Auf welche Weise wurde dieser bzw. ein vergleichbarer „Mechanismus“ bei der diesjährigen Übung getestet?

Wie bei jeder Übung wurden durch entsprechend gewählte Szenarioelemente und Spieleinlagen bestimmte Mechanismen (z. B. Alarmierungsschritte, Verschlüsselung, Vorgehensweisen) ausgelöst und deren Praktikabilität im „gespielten“ Krisenfall getestet. Dabei wird während der Übungsplanung ausgehend vom jeweiligen Übungszielelement eine gewünschte/erwartete Reaktion des Krisenstabs oder des Spielers abgeleitet. Hierzu wird dann ein Szenario-Element/fiktives Übungsereignis/auslösende Einspielung (z. B. Mail, Webartikel, Anruf, technische Vorfallsbeschreibung), passend zur gespielten Gesamtlage erstellt und zum gewünschten Zeitpunkt während der Übung eingespielt. Dann wird die Reaktion des Krisenstabs oder des Spielers auf die Einspielung beobachtet, dies mit der erwarteten Reaktion verglichen und in der Übungsauswertung dann besprochen.

9. Welche Konferenzen zu „Cybersicherheit“ haben auf Ebene der Europäischen Union in den Jahren 2011 und 2012 stattgefunden?

Der Bundesregierung liegen folgende Kenntnisse zu Konferenzen zu „Cybersicherheit“ in den Jahren 2011 bis 2012 vor:

European Union Ministerial Conference on Critical Information Infrastructure Protection, Balatonfüred, 14. bis 15. April 2011 (im Folgenden „Konferenz“ oder „Ministerkonferenz“ genannt)

a) Welche Tagesordnung bzw. Zielsetzung hatten diese jeweils?

Die Konferenz beschäftigte sich mit dem Schutz der europäischen kritischen Informationsinfrastrukturen. Im Mittelpunkt der Beratungen stand die Mitteilung der Europäischen Kommission über den Schutz kritischer Informationsinfrastrukturen „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit“ (KOM(2011) 163). Die Konferenz wurde in Fortsetzung des sogenannten Tallinn-Prozesses ausgerichtet, welcher 2009 durch ein EU-Ministertreffen zu dieser Thematik initiiert wurde.

b) Wer hat diese jeweils organisiert und vorbereitet?

Die Konferenz wurde vom ungarischen Ministerium für nationale Entwicklung in Zusammenarbeit mit der Europäischen Kommission organisiert und vorbereitet. Sie fand unter der Schirmherrschaft der ungarischen EU-Ratspräsidentschaft statt.

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 Kenntnisstand der Bundesregierung waren staatliche Vertreter von EU-Drittstaaten nicht aktiv an der Durchführung der Konferenz beteiligt, befanden sich aber möglicherweise unter den Teilnehmern (die Teilnehmerliste liegt der Bundesregierung nicht vor).

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

Auf der Konferenz war Deutschland mit einer Delegation bestehend aus Mitarbeitern des Bundesministeriums des Innern, des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesministeriums für Wirtschaft und Technologie (BMWi) vertreten. Private Einrichtungen waren in der deutschen Delegation nicht vertreten.

f) Welche weiteren privaten Akteure waren auf den Konferenzen anwesend?

Neben staatlichen Vertretern leisteten auch geladene Unternehmensvertreter als Vortragende oder Teilnehmer an Podiumsdiskussionen einen aktiven Beitrag zum Konferenzprogramm (z. B. von Nokia Siemens Networks, Microsoft oder Deutsche Telekom).

EU Cyber Security Conference, Brüssel, 6 Juli 2012

Zu Frage 9a
Die EU Cyber Security Conference wurde ausgerichtet mit dem Ziel, einen Meinungsaustausch zwischen der EU und den Mitgliedstaaten zur geplanten Europäischen Cyber-Sicherheitsstrategie durchzuführen. Im Kern der Diskussionen standen die Themen Sicherung der Wettbewerbsfähigkeit der Europäischen Union (EU) durch Netz- und Informationssicherheit, Stärkung der inneren Sicherheit durch Bekämpfung von Cybercrime sowie Cybersicherheit im Kontext der internationalen Politik und der Gemeinsamen Außen- und Verteidigungspolitik der EU.

Zu Frage 9b
Die Konferenz wurde gemeinsam von der Europäischen Kommission und dem Europäischen Auswärtigen Dienst organisiert.

Zu den Fragen 9c und 9d
Es waren keine Behörden der USA oder anderer Nichtmitgliedstaaten an der Konferenz beteiligt.

Zu Frage 9e
Die Bundesrepublik Deutschland war durch Mitarbeiter des Auswärtigen Amtes, des BMWi, des BMI und des BSI vertreten. Private Einrichtungen waren nicht an der Konferenz beteiligt.

Zu Frage 9f
Private Einrichtungen waren auf der Konferenz nicht anwesend.

First International Conference Cyber Crisis Cooperation: Cyber Exercises, Paris, 27. Juni 2012

Zu Frage 9a
Die Zielsetzung dieser Konferenz war ein Erfahrungsaustausch über die internationale Kooperation während Cyberkrisen mit speziellem Fokus auf Übungen in diesem Bereich.

Zu Frage 9b
Die Konferenz wurde von ENISA organisiert.

Zu den Fragen 9c und 9d
Vertreter aus den USA und Japan beteiligten sich mit Vorträgen über die von ihren Behörden organisierten Übungen und Techniken zur Übungsunterstützung.

Zu Frage 9e
Auf der Konferenz war Deutschland durch Mitarbeiter/-innen des BSI vertreten. Private Einrichtungen waren an der Konferenz nicht beteiligt.

Zu Frage 9f
Ein Großteil der Teilnehmer kam aus dem Behördenumfeld. Einige Teilnehmer stammten aus der Privatwirtschaft. Die Firma Crisis Plan beispielsweise wurde von ENISA zur Organisation von Cyber Europe 2012 beschäftigt.

10. An welchen der Konferenzen hat die Polizeiagentur Europol mit welchen Aufgaben teilgenommen?

    Welche Ergebnisse brachte der gemeinsame Workshop von Europol und der früheren polnischen Ratspräsidentschaft zur Erarbeitung der „Operational Action Plans“ bezüglich Cybersicherheit?

Europol hat gemeinsam mit den jeweils federführenden Staaten zur Vorbereitung der Operational Actions Plans (OAP) für das Jahr 2013 Workshops durchgeführt. Ein OAP zu Cybersicherheit ist der Bundesregierung nicht bekannt, weitergehende Informationen zu den Workshops liegen der Bundesregierung nicht vor.

11. Mit welchem Ziel sollen bei Europol eine „Virtual Task Force on Violent Extremism“ und ein „Portal on Violent Extremism“ eingerichtet werden, und woraus bestehen diese?

Im Rahmen der Virtual Task Force on Violent Extremism (TFVE) sollen Experten der Mitgliedstaaten über die Anpassung einer EU-weiten Strategie zur Erkennung und Bekämpfung des gewalttätigen Extremismus beraten. Ziel ist die Schaffung eines einheitlichen Instruments zur Harmonisierung entsprechender Maßnahmen auf Grundlage europäischer Rechtsnormen. Der reguläre Kontakt zwischen den Mitgliedern der TFVE soll über die „Europol Platform for Experts (EPE)“ durchgeführt werden. Der Austausch von operativen Informationen ist hierbei nicht vorgesehen.

Ein „Portal on Violent Extremism“ ist im Europol-Review genannt (www.europol.europa.eu/sites/default/files/publications/europolreview2011.pdf), zu einer Realisierung ist der Bundesregierung aber nichts bekannt.

12. Welche Zielsetzung hat die „Cybercrime Training and Education Group“ (ECTEG), und wer gehört ihr an?

Die European Cybercrime Training and Education Group (ECTEG) besteht seit 2001 und hat sich zum Ziel gesetzt, ein einheitliches Cybercrime Training zu

entwickeln und allen Strafverfolgungsbehörden der EU zur Verfügung zu stellen.

Full members sind die Strafverfolgungsbehörden der 27 EU-Mitgliedstaaten, Europol und CEPOL. Associate members sind Polizeien von Drittstaaten wie zum Beispiel Norwegen, Schweiz und der Türkei sowie Universitäten.

a) Welche Aufgabe übernehmen private Firmen in der ECTEG?

Die Cybercrime Trainingsmodule werden in Zusammenarbeit mit der Wissenschaft (Universitäten) und der Industrie entwickelt, um eine qualitativ hochwertige Fortbildung mit aktuellen Inhalten anbieten zu können. Dabei stellen private Firmen auch Trainer zur Verfügung (z. B. Microsoft).

b) Mit welchem Personal sind Behörden der Bundesregierung an der ECTEG beteiligt?

Das Bundeskriminalamt (BKA) ist seit 2008 aktives Mitglied der ECTEG.

13. Welche Zielsetzung hat die „European Union Cybercrime Task Force“ (EUCTF), und wer gehört ihr an?

In der European Cybercrime Task Force (EUCTF) arbeiten die mit der Bekämpfung von „Cybercrime“ befassten Dienststellen der Mitgliedstaaten mit der High Tech Crime Unit von Europol sowie Vertretern der Europäischen Kommission und Eurojust zusammen. Neben der Intensivierung des Informationsaustauschs im Bereich der Cybercrime ist die Unterstützung bei der Entwicklung von Strategien zur effektiven Bekämpfung von Cybercrime Gegenstand der Arbeit.

a) Welche Aufgabe übernehmen private Firmen in der EUCTF?

Nach Kenntnis der Bundesregierung haben private Firmen in der EUCTF keine Aufgaben übernommen.

b) Mit welchem Personal sind Behörden der Bundesregierung an der EUCTF beteiligt?

Das BKA ist in der EUCTF durch Mitarbeiter der Fachdienststelle zur Bekämpfung von Cybercrime vertreten.

14. Mit welchem Personal und Ausrüstung haben Behörden der Bundesregierung an den von Europol koordinierten Operationen „Crossbill“, „Mariposa II“, „Rescue“ und „Icarus“ teilgenommen?

a) Welches Ziel verfolgten die Operationen?

Operation „Icarus“
Als Ergebnis von Ermittlungen der dänischen Polizei im September 2011 im Zusammenhang mit dem Besitz und der Verbreitung kinderpornografischen Materials im Internet wurden insgesamt 269 verdächtige Personen in 22 Staaten identifiziert. Die Operation wurde durch Europol koordiniert und begleitet. Die deutsche Polizei, das BKA mit Unterstützung der Länderpolizeien, hat im Rahmen der Bearbeitung der 20 an Deutschland übermittelten Hinweise zehn Personen identifiziert. Die vergleichsweise geringe Identifizierungsrate ist auf die in Deutschland nicht gesetzlich geregelte Mindestspeicherung für IP-Adressen zurückzuführen. Bei neun der zehn Verdächtigen erfolgten in Deutschland ope-

rative Maßnahmen. Ein Verdächtiger war französischer Staatsangehöriger. Der Vorgang wurde an die französischen Behörden abgegeben. Die aktuellen Ermittlungsstände bei den Länderpolizeien liegen dem BKA derzeit nicht vor.

Operation „Rescue“
Bei der Operation „Rescue“ handelt es sich gleichfalls um eine von Europol initiierte Operation. Sie hatte ihren Ursprung bei den niederländischen Behörden und bezog sich auf eine Webseite, die als Portal für Personen mit sexuellem Interesse an Kindern (speziell Jungen) diente. Das Portal zählte zum Zeitpunkt seiner Feststellung 2011 ca. 60 000 registrierte Nutzer. An der Operation waren außer Europol, deutsche, französische, niederländische, britische und US-amerikanische Behörden beteiligt. Das BKA führte die Ermittlungen wegen Verdachts des sexuellen Missbrauchs von Kindern und der Verbreitung von kinderpornografischem Material. Grundlage des Verfahrens war der Austausch von Material und Gesprächen in dem oben bezeichneten Portal. Der Teilbereich, der Deutschland betraf, wurde als Ermittlungsverfahren gegen Unbekannt bei der Generalstaatsanwaltschaft Frankfurt/Main (ZIT) anhängig gemacht. Zum Zwecke der Beweiserhebungen wurden ca. 400 Forenbeiträge gesichtet und auf strafrechtliche Relevanz geprüft. In Deutschland wurden die Täter zu acht konkreten Verdachtsfällen ermittelt. In vier Fällen kam es zu weiteren operativen Maßnahmen.

b) Welche Ergebnisse erzielten die Operationen, und wie wurden diese von den Beteiligten bewertet?

Beide Operationen hatten ein international koordiniertes Vorgehen gegen Straftäter im Bereich des sexuellen Missbrauchs von Kindern zum Ziel. Da Straftaten im Internet nicht an Staatsgrenzen halt machen, ist eine internationale Bekämpfung und Vernetzung der Verfolgungsbehörden unabdingbar und mittlerweile Gegenstand der täglichen polizeilichen Arbeit. Grundsätzlich sind solche Operationen positiv zu bewerten, jedoch sind die jeweiligen Erfolgsmöglichkeiten von verschiedenen Faktoren abhängig (z. B. von den gesetzlichen und technischen Möglichkeiten und dem Fachwissen in den einzelnen an den Operationen teilnehmenden Behörden).

Zu den Operationen „Crossbill“ und „Mariposa“ liegen der Bundesregierung keine Informationen vor.

15. Worum geht es bei dem von Europol angeführten „Project 2020“?

Im „Projekt 2020“ will Europol nach Kenntnis der Bundesregierung die Trends im Bereich Cybercrime untersuchen und eine Prognose der Entwicklung für die nächsten acht Jahre erstellen.

a) Welche Behörden, Verbände, Wissenschaftler/-innen und Firmen sind in die Entwicklung von „Project 2020“ eingebunden?

Am Projekt nehmen nach Kenntnis der Bundesregierung neben Europol die „City of London police“, die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA), Experten des International Information System Security Certification Consortium (ISC) und der International Association of Public Prosecutors teil. Aus dem Bereich der Privatwirtschaft nehmen außerdem Visa Europe, Shop Direct Group, Transactis, Yodel, McAfee, CGI Canada, Atosm Cassidian, Digiware, Core Security Technologies und Trend Micro teil.

b) Welche Treffen haben nach Kenntnis der Bundesregierung zum „Project 2020“ stattgefunden, und welche Mitglieder der Bundesregierung nahmen daran teil?

Hierzu liegen der Bundesregierung keine Informationen vor, Mitglieder der Bundesregierung sind am Projekt nicht beteiligt.

c) Mit welchen Aufgaben sind Europol, die City of London Police, die Europäische Agentur für Netz- und Informationssicherheit (ENISA) und die International Association of Public Prosecutors am „Project 2020“ beteiligt?

d) Mit welchen Aufgaben ist die European Aeronautic Defence and Space Company (EADS) mit Cassidian am „Project 2020“ beteiligt, und wie unterscheidet sich dies von der Teilnahme übriger Hersteller von Anti-Virus-Produkten?

Hierzu liegen der Bundesregierung keine Informationen vor.

e) Inwieweit ist geplant, „Project 2020“ in eine permanente Einrichtung bzw. ein permanentes Netzwerk zu überführen?

Solche Pläne sind der Bundesregierung nicht bekannt.

16. Inwieweit hat sich Europol bisher auch mit dem Phänomen „Hacktivism“ beschäftigt?

Europol hat aufgrund von Straftaten in mehreren Mitgliedstaaten, die dem Bereich des sog. Hacktivism zugerechnet wurden, ein Arbeitstreffen durchgeführt, um die verschiedenen Ermittlungsverfahren zu koordinieren und das weitere Vorgehen zu planen. Die Ergebnisse werden nach Kenntnis der Bundesregierung derzeit noch ausgewertet.

a) Welche Treffen haben zu den Protesten von „Anonymous“, „Lulzsec“ oder „Antisec“ sowie anderen virtuellen Protesten stattgefunden?

b) Inwieweit ist Europol mit der Koordination entsprechender Ermittlungen der EU-Mitgliedstaaten befasst?

c) Mit welchem Personal und welcher Zielsetzung sind deutsche Behörden daran beteiligt?

d) Welche weiteren Maßnahmen sind hierzu geplant?

e) Welche Berichte hat Europol zum Komplex „Hacktivism“, „Anonymous“, „Lulzsec“ oder „Antisec“ zu welchem Zeitpunkt verfasst?

f) Wie und mit welchen Inhalten haben deutsche Behörden dazu beigetragen?

Weitere Aktivitäten von Europol im Phänomenbereich „Hacktivism“ sind der Bundesregierung nicht bekannt.

17. Welchen Stand haben die Verhandlungen um die Erweiterung des Mandates der ENISA?

Inwieweit hat die ENISA 2012 etwa im Rahmen von Workshops EU-Mitgliedstaaten bei der Planung nationaler „Krisenübungen“ unterstützt, und worin bestand die Unterstützung genau?

Der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ENISA steht im Rahmen des ordentlichen Gesetzgebungsverfahrens zur Ersten Lesung im Europäischen Parlament an.

Derzeit werden Verhandlungen über das Dossier zwischen der Ratspräsidentschaft, Vertretern des Europäischen Parlaments und der Europäischen Kommission im Rahmen informeller Triloge geführt. Dazu verlieh der Ausschuss der Ständigen Vertreter (1. Teil) in seiner Sitzung am 17. Oktober 2012 der zyprischen Ratspräsidentschaft ein allgemeines Mandat zur Aufnahme der Verhandlungen im Trilog. Die zyprische Präsidentschaft hat zwei Triloge durchgeführt. Die Verhandlungen werden mit der irischen Präsidentschaft (ab 1. Januar 2013) fortgeführt.

Der Bundesregierung sind keine ENISA-Workshops zur Unterstützung bei der Planung nationaler „Krisenübungen“ bekannt.

18. Welchen Stand hat der Aufbau eines „Europäischen Informations- und Warnsystems“ (EISAS), und wie beteiligt sich die Bundesregierung daran?

Welche Stellen innerhalb der EU sollen nach gegenwärtiger Planung der Europäischen Kommission an das EISAS angeschlossen sein?

Nach Kenntnis der Bundesregierung befindet sich das „Europäische Informations- und Warnsystem“ (EISAS) weiter im Stadium der Machbarkeitsüberprüfung. Die Bundesregierung ist daran nicht beteiligt.

Über den gegenwärtigen Planungsstand der Europäischen Kommission, welche Stellen innerhalb der EU an EISAS angeschlossen werden sollen, besitzt die Bundesregierung keine Kenntnis.

19. Mit welcher Zielsetzung nehmen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur an der „Europäischen öffentlich-privaten Partnerschaft für Robustheit“ (EP3R) teil, und welche Arbeiten werden dort übernommen?

Das BSI nimmt an der EP3R teil, um Arbeiten, die das BSI betreffen, dort zu begleiten. Das Gleiche gilt für die Bundesnetzagentur, welche im Auftrag des BMWi teilnimmt. Das BSI und die Bundesnetzagentur nehmen an Arbeitsgruppen teil. Es wurden bisher keine weiterführenden Aufgaben übernommen.

a) Welche Arbeitsgruppe oder Unterarbeitsgruppen existieren innerhalb des EP3R?

Bisher existieren drei Arbeitsgruppen:

Working Group 1:
Key assets, resources and functions for the continuous and secure provisioning of electronic communications across countries.

Working Group 2:
Baseline requirements for the security and resilience of electronic communications.

Working Group 3:
Coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications.

b) Welche Treffen haben hierzu in den letzten beiden Jahren stattgefunden, und wer nahm daran teil (bitte Behörden und private Firmen sowie Banken nennen)?

In den Jahren 2011 und 2012 haben bisher sieben Treffen stattgefunden, ein weiteres findet noch im Dezember 2012 statt. Teilnehmende Behörden sind das

BMI, das BSI und die Bundesnetzagentur. Des Weiteren nimmt der eco-Verband regelmäßig an den Sitzungen teil, deutsche Banken sind nach BSI-Kenntnisstand nicht vertreten.

c) Wer hat die Treffen jeweils vorbereitet?

Die Treffen werden von ENISA vorbereitet und durchgeführt, teilweise mit Unterstützung der Europäischen Kommission (DG CONNECT).

d) Welche Tagesordnung hatten die Treffen, und welche Verabredungen wurden jeweils getroffen?

Die Tagesordnungen enthielten die Themen der jeweiligen Arbeitsgruppen. Zudem gab es immer Sachstandsberichte von ENISA und der Europäischen Kommission. Vereinzelt wurden Firmenpräsentationen oder Vorstellungen von Studienergebnissen in die Veranstaltungen mit aufgenommen.

e) Auf welche Art und Weise ist es innerhalb des EP3R möglich, an den Aktivitäten der EU-USA-Kooperation mitzuwirken?

Die Europäische Kommission berichtet im EP3R über die EU-USA-Aktivitäten. Es besteht die Möglichkeit, dies zu kommentieren.

20. Mit welcher Zielsetzung nehmen das BSI und die Bundesnetzagentur am „Europäischen Forum der Mitgliedstaaten“ (EFMS) teil, und welche Arbeiten werden dort übernommen?

Das BSI und Bundesnetzagentur nehmen am EFMS teil, um die deutschen Interessen zu vertreten und die die Behörden betreffenden Arbeiten dort zu begleiten. Es wurden bisher keine weiterführenden Aufgaben im EFMS übernommen.

a) Welche Arbeitsgruppe oder Unterarbeitsgruppen existieren innerhalb des EFMS?

Das EFMS hat keine Arbeitsgruppen oder Unterarbeitsgruppen.

b) Welche Treffen haben hierzu in den letzten beiden Jahren stattgefunden, und wer nahm daran teil (bitte Behörden und private Firmen sowie Banken nennen)?

In den Jahren 2011 und 2012 haben bisher sechs Treffen stattgefunden, eines findet noch im Dezember statt. Das EFMS ist nur für Behörden zugänglich, aus Deutschland haben das BMI, das BSI und die Bundesnetzagentur teilgenommen.

c) Wer hat die Treffen jeweils vorbereitet?

Die Treffen werden von der Europäischen Kommission vorbereitet, teilweise mit Unterstützung von ENISA.

d) Welche Tagesordnung hatten die Treffen, und welche Verabredungen wurden jeweils getroffen?

Die Tagesordnungen orientierten sich an den jeweils aktuellen Themen der Kooperation der Mitgliedstaaten zum Schutz kritischer Informationsinfrastrukturen. Themen waren beispielsweise die EPCIP-Richtlinie, EU-Übungen, die EU-USA-Kooperation, Sachstandsdarstellungen aus den Mitgliedstaaten, die Cyber-Sicherheitsstrategie der EU, der Europäische Cyber-Sicherheitsmonat,

Initiativen zum Informationsaustausch sowie Aktivitäten der Europäischen Kommission zum Informationsaustausch mit Drittstaaten. Konkrete Verabredungen wurden nicht getroffen, da das EFMS ein Gremium für den Informationsaustausch ist und über keine Entscheidungskompetenzen verfügt.

e) Auf welche Art und Weise ist es innerhalb des EFMS möglich, an den Aktivitäten der EU-USA-Kooperation mitzuwirken?

Im EFMS werden Planung und Fortschritte auf der EU-USA-Kooperation vorgestellt. Im Rahmen des EFMS besteht die Möglichkeit, die Planungen zu kommentieren und so Einfluss auf Entscheidungen und den weiteren Projektverlauf zu nehmen.

21. Welche neuen Erkenntnisse hat die Bundesregierung darüber, wo es im Jahr 2012 einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat?

Zu versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlägen“ liegen der Bundesregierung keine Erkenntnisse vor.

22. Inwieweit verfügt die Bundesregierung mittlerweile über neue Hinweise zur Urheberschaft der Computerviren „Stuxnet“ und „Flame“?

Dem BSI liegen keine eigenen Hinweise zur Urheberschaft der Computerviren „Stuxnet“ und „Flame“ vor.

a) Welche eigenen Erkenntnisse hat die Bundesregierung über „Stuxnet“ und „Flame“ gesammelt?

Komplexität und Wirkungsweise dieser Computerviren lassen auf höchste Professionalität mit großen personellen und finanziellen Ressourcen schließen.

b) Hat die Bundesregierung eine Analyse dieser Schadsoftware extern oder intern in Auftrag gegeben?

Das BSI hat eine externe Firma mit der Analyse der genannten Schadsoftware beauftragt. Das BSI hat im Rahmen seines gesetzlichen Auftrags technische Informationen über die Wirkungsweise der beiden Schadprogramme gesammelt und diese ausgewertet.

c) Welche Erkenntnisse über diese Schadsoftware hat die Bundesregierung von anderer Seite erhalten?

Das BSI (CERT-Bund) hat durch seine nationalen und internationalen Kontakte technische Details zum Verhalten und zu Rückmeldekanälen der Schadsoftware, sowie über die weltweite Verteilung von infizierten Systemen erhalten.

d) Hat die Bundesregierung, angesichts der Tatsache, dass für die Programmierung von „Stuxnet“ detaillierte Kenntnisse des Steuerungssystems PCS-7 nötig waren, Hinweise, wie diese in Umlauf geraten sind?

e) Ist die Bundesregierung zur Klärung dieser Frage an die Firma Siemens AG herangetreten, deren Produkte von „Stuxnet“ betroffen sind, und welche Kenntnisse hat sie dabei gewonnen?

Die Bundesregierung ist zur Klärung dieser Frage an die Siemens AG herangetreten. Grundsätzlich ist die Programmierung von Steuerungssystemen ausgiebig durch die Hersteller dokumentiert. Es gibt weltweit eine Vielzahl von Entwicklern, die über entsprechende Kenntnisse verfügen.

f) Welche Schlussfolgerungen zieht die Bundesregierung diesbezüglich für die Sicherheit jener Industrieanlagen in Deutschland, die das Steuerungssystem PCS-7 nutzen?

Die Siemens AG hat Empfehlungen für die sichere Konfiguration des Steuerungssystems PCS-7 veröffentlicht. Die Umsetzung der Empfehlungen inklusive Patch-Management eingesetzter Software-Produkte und der Einsatz weiterer Sicherheitsprodukte bietet einen nach dem Stand der Technik ausreichenden Schutz. Zusätzlich gibt es Empfehlungen des BSI zu grundlegenden Schutzmaßnahmen für Kontrollsysteme. Zum Schutz der Kritischen Infrastrukturen vor IT-Ausfällen hat der Bundesminister des Innern im Jahre 2012 Gespräche mit den Betreibern kritischer Infrastrukturen geführt. Derzeit befinden sich gesetzliche Maßnahmen in der Prüfung.

23. Welche „best practices“ existieren hinsichtlich der Verhinderung einer „illegalen Nutzung“ bzw. „terroristischen Nutzung“ des Internets in Deutschland?

Die Nutzung des Internets zu rechtswidrigen Zwecken in Deutschland kann nicht allein durch Strafverfolgungs- bzw. Sicherheitsbehörden verhindert werden. Nur gesamtgesellschaftliche Ansätze können eine effektive Verhinderung solcher Nutzung, insbesondere im terroristischen Zusammenhang gewährleisten. Als „best practices“, an denen staatliche Stellen beteiligt sind, werden in diesem Sinne Kooperationen mit Partnerbehörden, Unternehmen, Nichtregierungsorganisationen und anderen Stellen, die mit dem Thema befasst sind, angestrebt und gegebenenfalls weiter ausgebaut (Beispiele: Mitwirkung am Projekt „Clean IT“, Aufbau von Präventionsforen, Zusammenarbeit mit Einrichtungen wie Jugendschutz.net).

Neben diesem gesamtgesellschaftlichen Ansatz haben sich die etablierten nationalen und internationalen polizeilichen und justiziellen Wege bewährt.

a) Welche weiteren „best practices“ sind zukünftig geplant?

„Best practices“ sind regelmäßig nicht planbar, sondern bilden sich aus verschiedenen Ansätzen heraus.

b) Welche Details dieser „best practices“ kann die Bundesregierung angeben hinsichtlich der Akteure, Aktionen, Regierungsführung, Kosten, Effekte?

„Best practices“ sind bereits begrifflich kein Bündel abgetrennter Maßnahmen, die im Rahmen einer isolierten Strategie verfolgt werden. Vielmehr werden „best practices“ gerade dadurch definiert, dass sie Vorgehensweisen im Rahmen der gewöhnlichen Tätigkeit von Behörden, Unternehmen oder Organisationen darstellen, die sich im Vergleich als besonders zielführend erwiesen haben und sich oftmals erst im Rahmen einer anstehenden Diskussion über ein bestimmtes Thema als mitteilenswert erweisen. Es besteht daher keine zentrale Katalogisierung solcher „best practices“.

c) Welche „terroristische Nutzung“ des Internets wird in Deutschland als problematisch angesehen?

Von extremistischen und terroristischen Gruppen „autorisierte“ Medienarbeit hat inzwischen für extremistische und terroristische Gruppierungen im Phänomenbereich des islamistischen Terrorismus eine herausragende Bedeutung und ist neben Anschlägen wesentlicher Teil der Aktivität terroristischer Gruppierungen. Das Internet ist hierbei inzwischen das entscheidende Leitmedium. Es bietet – zumeist als einziges den Gruppen zur Verfügung stehendes relevantes Medium – die Möglichkeiten, schnell und weltumspannend eine Vielzahl von Gleichgesinnten zu erreichen, virtuell zu missionieren, zu mobilisieren, zu radikalisieren oder gar zu rekrutieren.

d) Welche Beispiele existieren, um diese zu begrenzen?

Hierzu wird als ein Beispiel auf die erfolgreichen Strafverfolgungsmaßnahmen verwiesen, in deren Rahmen Personen, die im Auftrag oder im Sinne terroristischer Gruppierungen sich deren Propaganda zu eigen gemacht haben und sie dann im Internet verbreitet haben. Zudem wird auf das Gemeinsame Internetzentrum und die Indizierungen terroristischer Inhalte durch die Bundesprüfstelle für jugendgefährdende Medien hingewiesen, die dafür gesorgt haben, dass die entsprechenden Inhalte in Suchmaschinenergebnissen nicht mehr angezeigt werden, sowie auf Vereinsverbote, die zur Schließung der Internetauftritte der dann verbotenen Vereine führten.

e) Welche deutschen Firmen, Provider, Behörden, Organisationen oder sonstigen Stellen würden aus Sicht der Bundesregierung Interesse haben, Einladungen zum „Clean IT“-Projekt zu erhalten?

Das „Clean IT“-Projekt wird im Januar 2013 mit einer öffentlichen Konferenz in Brüssel zum Abschluss gelangen und zuvor sind keine Treffen mehr geplant. Einladungen zum „Clean IT“-Projekt werden daher nicht mehr ausgesprochen.

24. Welche Schlussfolgerungen zieht die Bundesregierung aus dem Bericht „The Use of the Internet for Terrorist Purposes“ des United Nations Office on Drugs and Crime (UNODC)?

Die Bundesregierung hat keine abgestimmte Auffassung zum Bericht gebildet.

a) Auf welche Art und Weise arbeiten Bundesbehörden mit dem UNODC hinsichtlich des Abhörens von Kommunikationstechnologie bzw. Rahmenbedingungen zusammen?

Eine solche Kooperation findet nicht statt. Das Auswärtige Amt hat in den Jahren 2011 und 2012 je einen von dem Büro der Vereinten Nationen für Drogen- und Verbrechenbekämpfung (UNDOC) veranstalteten Workshop zum Thema „Countering the Use of he Internet for Terrorist Purposes“ mit Projektmitteln gefördert. Der Schwerpunkt des Vorhabens lag auf der Implementierung vorhandener Rechtsgrundlagen im internationalen Rahmen zur Vorbeugung und Verfolgung der Benutzung des Internets zur Vorbereitung und Ausführung von Terrorakten.

b) Inwieweit teilt die Bundesregierung die im Bericht geäußerte Auffassung, dass ein „international anerkanntes Abkommen über die Speicherung von bei Internet-Providern gesammelten Daten“ fehle (www.gulli.com/news/20029-un-fordert-internet-ueberwachung-zur-terrorismus-bekaempfung-2012-10-22)?

Die Bundesregierung hat sich hierzu keine Auffassung gebildet.

c) Sollten nach Ansicht der Bundesregierung wie im UNODC-Bericht beschrieben auch Anbieter von Instant Messaging und Internettelefonie (VoIP) Logs der über den Dienst geführten Gespräche archivieren?

Die Bundesregierung hat sich hierzu noch keine abschließende Meinung gebildet.

d) Auf welche Art und Weise hat die Bundesregierung zum Bericht „The Use of the Internet for Terrorist Purposes“ beigetragen?

Am 25. und 26. Januar 2009 nahm ein Referent des BMI an einem CITIF-Workshop mit dem Titel „Countering Terrorist Use of the Internet – Addressing Legal Aspects“ zum fachlichen Austausch teil, dessen Ergebnisse als Vorarbeit zu dem UNODC-Bericht dienten. Vonseiten des BKA nahm ein wissenschaftlicher Mitarbeiter des kriminalistischen Instituts an der Sitzung vom 5. bis 6. Oktober 2012 zur Erstellung des VN-Berichts zur Verwendung des Internets für terroristische Zwecke in Wien teil.

e) Welche Empfehlungen oder Anregungen für den Report „The Use of the Internet for Terrorist Purposes“ wurden dem UNODC übermittelt?

Dem UNODC wurden keine Empfehlungen oder Anregungen der Bundesregierung übermittelt. Soweit ein fachlicher Austausch in den genannten Gesprächen stattfand, ist dieser nicht nachvollziehbar.

25. Inwieweit existiert ein „Notfallplan“ des Bundes für den Fall eines großangelegten IT-Angriffs oder Störungen anderer Art?

a) Wenn ja, was sind die Eckpunkte dieses Notfallplans?

b) Wenn nicht, warum nicht?

Das IT-Krisenmanagement setzt auf die existierenden Mechanismen und Maßnahmen des allgemeinen Krisenmanagements auf. Eine zentrale Rolle bei der Bewältigung von IT-Krisen spielt dabei das Nationale Cyber-Abwehrzentrum, das IT-Vorfälle bewertet und Handlungsempfehlungen ausspricht. Das BSI mit den zuständigen Entitäten CERT-Bund, IT-Lagezentrum und IT-Krisenreaktionszentrum unterstützt dabei. Festgestellte groß angelegte IT-Angriffe oder Störungen anderer Art werden bewertet und Betroffene bei der Bewältigung mit konkreter technischer Hilfestellung unterstützt. Dabei wird mit den zuständigen Stellen in der öffentlichen Verwaltung, den kritischen Infrastrukturen, der Wirtschaft und den Bürgern jeweils geeignet zusammengearbeitet. Die Reaktionsfähigkeit zur Krisenbewältigung wird von der Bundesverwaltung in Zusammenarbeit mit den Ländervertretungen regelmäßig geübt. Im Rahmen des Umsetzungsplans KRITIS arbeitet das BSI bereits seit 2007 auf kooperativer Basis mit zahlreichen Vertretern kritischer Infrastrukturen zusammen, übt regelmäßig die Abwehr von IT-Sicherheitsvorfällen und Kommunikationswege und erarbeitet mögliche Krisenreaktionsmaßnahmen.

26. Wie wurde die privatwirtschaftliche Entwicklung oder Forschung in den Bereichen IT-Sicherheit und IT-abhängige „kritische Infrastruktur“ seit 2009 durch den Bund gefördert (bitte aufschlüsseln nach Jahr, Art der Förderung, finanzielle Mittel, beteiligte Firmen)?

Das Bundesministerium für Bildung und Forschung (BMBF) fördert im Bereich „Kommunikationssysteme; IT-Sicherheit“ seit 2010 26 Verbundprojekte und drei Kompetenzzentren mit insgesamt 104 Partnern aus Hochschulen, Forschungseinrichtungen und Industrie mit einem Gesamtfördervolumen von rund 47,5 Mio. Euro. Eine Liste der Industriepartner ist beigefügt (siehe Anlage).

a) Welche Forschungen finden hierzu im Auftrag des Bundes statt?

Im obigen Zusammenhang ist nur das IT-Sicherheitsforschungsprogramm des BMBF bekannt. Im Jahr 2008 haben sich das BMI und das BMBF auf ein gemeinsames IT-Sicherheitsforschungsprogramm verständigt. Vier Schwerpunkte des Arbeitsprogramms wurden über Ausschreibungen (Zeitraum 2009 bis 2011) abgedeckt. Diese sind:

– Sicherheit in unsicheren Umgebungen
– Schutz von Internet-Infrastrukturen
– Eingebaute Sicherheit
– Neue Herausforderungen zum Schutz von IT-Systemen und der Identifikation von Schwachstellen.

Die Projekte laufen zum größten Teil (siehe oben) bzw. befinden sich in der Bewilligungsphase. Die Zuständigkeit liegt beim BMBF.

b) Welche Art von Forschung oder Entwicklung wird hierzu seitens der Bundeswehr betrieben?

Die Bundeswehr realisiert im Bereich der IT-Sicherheit anwendungsnahe Forschungs- und Technologievorhaben ausschließlich für eigene Zwecke.

Eine Förderung der Privatwirtschaft auf diesem Gebiet in Form von Zuwendungen erfolgt nicht.

27. In wie vielen Fällen leistete das Bundesamt für Sicherheit in der Informationstechnik Unterstützung nach § 3 Absatz 13 des BSIG-Gesetzes (BSIG) seit Inkrafttreten des Gesetzes (bitte aufschlüsseln nach Datum, vorgeworfene Straftat auf Grund derer Daten gesammelt wurden, erhobene Anklagen und rechtskräftige Verurteilungen, die u. a. aufgrund der Analyse des BSI zustande kamen sowie der jeweiligen Behörde, die vom BSI unterstützt wurde)?

Seit Inkrafttreten des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes im Jahre 2009 wurden 131 (2009: 24, 2010: 45, 2011: 46, 2012: 16) Unterstützungsersuchen der Polizeien und Strafverfolgungsbehörden bearbeitet. Es wurde zu folgenden Delikten unterstützt: Eigentumsdelikte (34 Fälle), Straftaten gegen das Leben (10), Landesverrat und Gefährdung der äußeren Sicherheit (8), Straftaten gegen die sexuelle Selbstbestimmung (10), Straftaten gegen die persönliche Freiheit (3), Verstoß gegen das Betäubungsmittel-Gesetz (2), Amtsdelikte (1) und Straftaten gegen die Öffentliche Ordnung (10). In 53 Fällen wurden keine Angaben zum Delikt gemacht. Hintergründe, etwa zu anschließenden strafrechtlichen Auswirkungen, sind dem BSI nicht bekannt.

Unterstützte das BSI im Rahmen des § 3 Absatz 13 BSIG Behörden in Fällen, die in Zusammenhang mit der rechtsextremen Gruppierung NSU bzw. entsprechenden Ermittlungen stehen oder standen, und wenn ja, welche, und in welchem Umfang?

Im Zusammenhang mit der rechtsextremen Gruppierung NSU hat das BSI keine Unterstützungsarbeit geleistet.

28. In welchem Umfang hat die Bundesregierung in den letzten fünf Jahren Exportkreditgarantien in Form von Hermesbürgschaften zur Absicherung der Ausfuhr von Waren und Dienstleistungen aus dem Bereich der

Telekommunikationstechnik übernommen (siehe Bundestagsdrucksache 17/8052; bitte als Tabelle mit Produkt, Hersteller/Herstellerin, Finanzvolumen des Auftrags bzw. der übernommenen Exportkreditgarantie, Datum und belieferter Behörde/Stelle darstellen)?

Seit 2008 wurden in folgendem Umfang Exportkreditgarantien für Lieferungen und Leistungen im Bereich Telekommunikationstechnik übernommen:

Jahr	Warenart	Land	Volumen in Mio. EUR
2008	Telekommunikationsgeräte	Algerien	8,6
		Jemen	15,2
		Kasachstan	31,8
		Kolumbien	10,5
	Mobil- und Funknetze	Pakistan	0,4
		Russland R.F.	38,0
2009	Telekommunikationsgeräte	Algerien	2,8
		Bangladesch	7,7
		Iran	1,8
		Pakistan	13,5
		Türkei	0,4
	Mobil- und Funknetze	Äthiopien	2,2
		Bangladesch	37,0
		Jemen	4,9
		Mexiko	1,4
		Pakistan	4,3
		Russland R.F.	15,1
		Senegal	0,1
		Vereinigte Arab. Emirate	156,0
	Leitungsnetze	Ägypten	8,5
2010	Telekommunikationsgeräte	Iran	0,2
		Pakistan	38,8
		Russland R.F.	3,4
	Mobil- und Funknetze	Brasilien	68,5
		Dubai, VAE	158,4
		Kuwait	6,0
		Libyen	0,3
		Pakistan	22,8
		Russland R.F.	25,8
		Tschechische Republik	0,3
		Tunesien	4,1
2011	Telekommunikationsgeräte	Irak	17,6
		Pakistan	22,9
		Peru	6,0
		Türkei	21,3
	Mobil- und Funknetze	Mexiko	0,9
		Pakistan	2,4
2012	Telekommunikationsgeräte	Ägypten	2,1
		Pakistan	0,5

a) Welche der gelieferten Anlagen oder Produkte erlauben nach Kenntnis der Bundesregierung auch eine Überwachung oder Unterbrechung der Telekommunikation?

Keine der gelieferten Anlagen oder Produkte erlauben nach Kenntnis der Bundesregierung eine Überwachung oder Unterbrechung der Telekommunikation.

b) In welchen Fällen musste die Exportkreditversicherung tatsächlich wegen Zahlungsausfällen eintreten?

Die staatliche Exportkreditversicherung musste in keinem der Fälle aufgrund eines Zahlungsausfalls eintreten.

c) In welchen Fällen wurde die beantragte Übernahme einer Hermesbürgschaft nicht gewährt?

Seit 2008 sind im Bereich der Telekommunikationstechnik in 23 Fällen Exportkreditgarantien nicht endgültig übernommen worden.

29. Welchen Stand hat der Vorschlag des früheren polnischen Ratsvorsitzes, auf EU-Ebene die Erstellung eines „Glossars“ mit einheitlichen Definitionen zu „Cyberbedrohungen“ zu erarbeiten?

a) Inwieweit wurde dies auch in „Anti-Terror-Arbeitsgruppen“ der EU behandelt?

b) Was ist damit gemeint, wenn die Bundesregierung davon spricht, die Arbeiten am Glossar sollten „auf Terroraspekte beschränkt werden“ (Bundestagsdrucksache 17/7578)?

Das Vorhaben wurde unter polnischer Ratspräsidentschaft innerhalb der Ratsarbeitsgruppe Terrorismus bearbeitet, von den nachfolgenden Ratspräsidentschaften jedoch nicht weiter verfolgt. Die Bundesregierung hatte sich dafür eingesetzt, die Arbeiten in der Ratsarbeitsgruppe Terrorismus auf Terroraspekte der Cyberbedrohungen zu beschränken, andere Facetten wie Cybercrime sollten ausgenommen sein.

30. Welche konkreten Vorschläge hatte der Rat der Europäischen Union an die „Internet Corporation for Assigned Names and Numbers“ (ICANN) gerichtet, um „die Vorschläge im Strafverfolgungsbereich zur Minderung der Missbrauchsgefahren“ im Internet umzusetzen (Bundestagsdrucksache 17/7578)?

Es wurden eine Reihe von Maßnahmen entwickelt, die die Eindämmung der Missbrauchsgefahr von Domainnamen bei der Erweiterung der Top-Level-Domains und beim Übergang zu IPv6-Adressen unterstützen sollen. Die Maßnahmen wurden in einem Dokument mit der Bezeichnung „Law Enforcement Recommendations Regarding Amendments to the Registrar Accreditation Agreement“ zusammengefasst, das auf der Internetseite der ICANN (www.icann.org) abrufbar ist. Die vorgeschlagenen Maßnahmen reichen von der Akkreditierung von Antragstellern vor der Vergabe neuer Domainnamen bis hin zur Bekanntmachung von Kontaktstellen in Fällen einer missbräuchlichen Verwendung.

31. Auf welche Art und Weise konnte die Löschung kinderpornographischer Internetinhalte „durch intensivere Zusammenarbeit der zuständigen Stellen verbessert werden“, wie es die Bundesregierung in ihrer Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 17/7578 erläutert?

Welche „zuständigen Stellen“ sind gemeint, und worin bestand ihre Aufgabe?

Zur Verbesserung der Löschung kinderpornographischer Internetinhalte haben sich das BKA, die Selbstregulierungseinrichtungen der Internetwirtschaft und jugendschutz.de sowie die Bundesprüfstelle für jugendgefährdende Medien auf eine enge Kooperation verständigt und die Grundlagen ihrer Zusammenarbeit schriftlich in einer Kooperationsvereinbarung fixiert. Insbesondere wurden die Meldewege zu und Meldeverfahren an Nichtregierungsorganisationen optimiert.

Dabei wird zur Beförderung von Löschbemühungen für im Ausland gehostete Angebote neben dem polizeilichen Weg auch auf das INHOPE-Netzwerk zurückgegriffen, dem die vorgenannten deutschen Internet-Beschwerdestellen angehören.

Bei im Ausland gehosteten Angeboten meldet das BKA die Hinweise über den Interpolweg an die zuständige Dienststelle im Standortland des Servers, verbunden mit einem Löschungsersuchen. Den Ersuchen wird in der Regel innerhalb weniger Tage entsprochen. Zudem werden dem BKA bekannt gewordene einschlägige Seiten parallel zur Übermittlung auf dem Interpolweg mit einem Löschungsersuchen an die jeweiligen INHOPE-Partner im Standortland des Servers übermittelt, auf dem die Angebote gehostet werden. Diese Aufgabe übernimmt jeweils jugendschutz.net.

Die Kooperationspartner jugendschutz.net, eco und die Freiwillige Selbstkontrolle Multimedia-Dienstanbieter (fsm) bieten ebenso wie das BKA und Landespolizeien die Möglichkeit für Bürger an, Hinweise auf Websites mit Missbrauchsdarstellungen an Kindern online zu melden. Soweit Hinweise bei den Beschwerdestellen eingehen, werden diese alle an das BKA weitergeleitet.

Die eingehenden Hinweise werden durch die Strafverfolgungsbehörden tagesaktuell bearbeitet.

Soweit in Deutschland gehostete Websites mit Missbrauchsdarstellungen an Kindern bekannt werden, entspricht es der gemeinsamen Erfahrung von BKA und Nichtregierungsorganisationen, dass die Inhalte regelmäßig binnen Tagesfrist nach Meldung an den Provider gelöscht werden.

32. Welches „technology monitoring tool“ hatte der Chef des Bundeskriminalamts (BKA) bei einer Sitzung der „European Police Chiefs Convention“ vorgestellt (Ratsdokument 16538/12)?

    a) Welche Tagesordnung hatte das Treffen der „European Police Chiefs Convention“, und wer hatte diese erstellt?

    b) Welche weiteren Beiträge wurden auf dem Treffen gehalten?

Zu dem im EU-Ratsdokument 16538/12 angeführten „technology monitoring tool“ referierte der Präsident des BKA über die technologische Früherkennung als Komponente einer ganzheitlichen Früherkennungsstrategie des BKA. Dazu wird auch auf Seite 14 f. des Vermerks zur „European Police Chiefs Convention“ in EU-Ratsdokument 11572/12 verwiesen.

Die Tagesordnung zur „European Police Chiefs Convention“ wurde von Europol erstellt. Im Übrigen wird zur Beantwortung dieser Fragen auf den umfangreichen Vermerk zur „European Police Chiefs Convention“ in EU-Ratsdokument 11572/12 verwiesen.

33. Inwieweit ist der wegen Fälschung seiner Doktorarbeit zurückgetretene, frühere Bundesminister der Verteidigung Karl-Theodor Freiherr zu

Guttenberg nach Kenntnis der Bundesregierung als Berater bzw. sonstiger Vertragsnehmer für Gremien oder Institutionen der EU hinsichtlich netzpolitischer Fragen aktiv?

a) Welche Leistungen wurden von ihm nach Kenntnis der Bundesregierung hierzu in den Jahren 2011 und 2012 erbracht?

b) Hat die Bundesregierung dieser Tätigkeit des früheren deutschen Bundesverteidigungsministers in einem EU-Gremium oder einer Arbeitsgruppe zugestimmt?

c) Falls ja, was bewog die Bundesregierung zur Auffassung, dass Karl-Theodor Freiherr zu Guttenberg für die Aufgabe geeignet wäre?

Nach Beendigung der Amtszeit als Bundesminister sieht das Gesetz über die Rechtsverhältnisse der Mitglieder der Bundesregierung (Bundesministergesetz) keine Einschränkungen oder Anzeigepflichten in Bezug auf die Ausübung eines neuen Amtes, Gewerbes oder Berufes vor. Der Bundesregierung liegen demnach keine amtlichen Erkenntnisse über netzpolitische Aktivitäten des ehemaligen Bundesministers der Verteidigung, Karl-Theodor Freiherr zu Guttenberg, vor. Aus diesem Grunde können die Fragen 33a bis 33c nicht beantwortet werden.

34. Ist der Bundesregierung bekannt, wo und inwiefern auf EU-Ebene über eine Nachfolge des „Stockholm-Programms“ diskutiert wird?

Welche Bestimmungen sollen in einem neuen Fünfjahresplan nach Ansicht der Bundesregierung hinsichtlich Cybersicherheit oder der Kontrolle des Internets besonders priorisiert werden?

Am 13. November hat die Ratspräsidentschaft eine Halbzeitbewertung des noch bis 2014 laufenden Stockholmer Programms vorgelegt. Im Rahmen der politischen Diskussion des JI-Rates am 6. und 7. Dezember 2012 sprachen sich einige Mitgliedstaaten für ein Nachfolgeprogramm zum Stockholmer Programm aus. Insbesondere Italien, dass zum Zeitpunkt des Auslaufens des Stockholmer Programms Ende 2014 die EU-Ratspräsidentschaft innehaben wird, zeigte sich an der Entwicklung eines Nachfolgeprogramms interessiert. Die Europäische Kommission zeigte sich zurückhaltend. Konkrete Fragen der Ausgestaltung wurden bislang aber nicht diskutiert.

Anlage

Zuwendungsempfänger	**Ort**
adesso mobile solutions GmbH	Dortmund
Alcatel-Lucent Deutschland AG	Stuttgart
Astaro GmbH & Co. KG	Mannheim
Avira Operations GmbH & Co. KG	Ulm
Collax GmbH	München
Controlware GmbH Kommunikationssysteme	Offenbach am Main
DE-CIX Management GmbH	Köln
DECOIT GmbH	Bremen
Deutsche Akademie der Technikwissenschaften e. V. (acatech)	München
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Kaiserslautern
DFN-CERT Services GmbH	Hamburg
Dr. Bülow & Masiak GmbH	Gelsenkirchen
EADS Deutschland GmbH	München
EANTC Aktiengesellschaft	Berlin-Charlottenburg
ERNW Enno Rey Netzwerke GmbH	Mannheim
escrypt GmbH Embedded Security	Bochum
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	München
G DATA Software AG	Bochum
GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH	München
Globalways AG	Stuttgart
GSMK Gesellschaft für sichere mobile Kommunikation mit beschränkter Haftung	Berlin
Hirschmann Automation and Control GmbH	Stuttgart
idalab GmbH	Berlin-Charlottenburg
Infineon Technologies AG	München
ISACO GmbH	Berlin-Charlottenburg
Kontron Europe GmbH	Kempten (Allgäu)
macmon secure gmbh	Berlin-Charlottenburg
N C P e GmbH Network Communications Products engineering	Nürnberg
Nokia Siemens Networks GmbH & Co. KG	München
Recurity Labs GmbH	Berlin-Charlottenburg
SCHUTZWERK GmbH	Memmingen
secunet Security Networks Aktiengesellschaft	Essen
Sirrix Aktiengesellschaft	Saarbrücken
Software Aktiengesellschaft	Darmstadt
SYSGO AG	Mainz
The unbelievable Machine Company GmbH	Berlin-Charlottenburg
ToasterNET GmbH	Fürth
Utimaco Safeware AG	Bad Homburg v. d. Höhe
Vodafone D2 GmbH	Düsseldorf

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