Deutscher Bundestag **Drucksache 17/7578**

17. Wahlperiode 02. 11. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/7118 –

Cyber-Übungen der Europäischen Union, der USA und die deutsche Beteiligung

Vorbemerkung der Fragesteller

Am 4. November letzten Jahres hatte die Europäische Union ihre erste europäische Cyber-Übung „Cyber Europe 2010“ begonnen, um eine Reaktion auf „Onlinebedrohungen“ zu testen. 22 Mitgliedstaaten beteiligten sich, die Übung wurde vom European Network and Information Security Agency (ENISA) mit Sitz in Athen organisiert. Mit den Übungen soll die ENISA an der Verbesserung einer „Abwehrbereitschaft der EU“ arbeiten und hierfür laut einer Mitteilung des Ausschusses Ständiger Vertreter (AStV) zur „Robustheit und Stabilität des Internets, zum Aufbau strategischer internationaler Partnerschaften und zur Einbringung koordinierter Beiträge in internationalen Foren“ beitragen (Ratsdokument 10299/11). Chef der ENISA ist Udo Helmbrecht, früherer Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Übungen wie „Cyber Europe“ adressieren auch Cyberkriminalität. Unklar bleibt, welche konkreten „Störungen“ außer „Distributed Denial of Service Attacks“ (DDoS) im Mittelpunkt stehen und welcher Art die Antworten von Behörden und Privatwirtschaft darauf sind. In einer Mitteilung vom 31. März 2011 zum „Schutz kritischer Informationsinfrastrukturen ‚Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit‘“ spricht die Europäische Kommission (im Folgenden: Kommission) von der Nutzung von Informations- und Kommunikationstechnologie (IKT) zur Erlangung „politischer, wirtschaftlicher und militärischer Macht“ bzw. „Cyberkrieg“ und „Cyberterrorismus“. Indes hat es bislang – soweit bekannt – noch keinen „cyberterroristischen“ Angriff gegeben.

Im Ratsdokument 10299/11 wird neben einer „nationalen, europäischen und globalen Kultur der Risikoanalyse und des Risikomanagements auf allen Ebenen“ die Entwicklung „koordinierter Maßnahmen zur Prävention, Erkennung und Eindämmung von Störungen aller Art und zur entsprechenden Reaktion“ genannt. EU-Mitgliedstaaten sollen „einander bei grenzüberschreitenden Sicherheitsvorfällen auf freiwilliger Basis“ gegenseitig Hilfe leisten. Gegenüber dem Internetportal www.heise.de äußerte ENISA-Chef Helmbrecht, mög-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 28. Oktober 2011 übermittelt.

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

liches Szenario einer zukünftigen „Cyber Europe“ seien „Angriffe auf das Netz am Bankenplatz in Frankfurt“.

Im April 2011 hatte die Kommission in Balatonfüred eine Ministerkonferenz über den „Schutz kritischer Informationsinfrastrukturen“ veranstaltet, deren Ergebnisse der Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft“ berichtet wurden. Gefordert wurde, die ENISA „rasch zu reformieren, zu modernisieren und zu verstärken“. Hierfür sollen vor allem die nationalen „IT Notfalldienste“ (Computer Emergency Response Teams – CERT) koordiniert werden, die sich zum großen Teil aus der Privatwirtschaft rekrutieren. Nahtlos werden dadurch die beteiligten Firmen in die „Ausarbeitung nationaler Notfallpläne für Netzstörungen sowie der Veranstaltung von nationalen Übungen zur Internetsicherheit“ integriert, um neben einer „Generierung von Wachstum“ auch zur „Wettbewerbsfähigkeit“ und „Schaffung von Arbeitsplätzen“ beizutragen. In Deutschland werden CERT unter anderem von einigen Bundesländern, aber auch der Bundeswehr, dem BSI, der Volkswagen AG, der Commerzbank AG, IBM, SAP, der Siemens AG und der Telekom Deutschland GmbH betrieben.

Kurz vor der „Cyber Europe 2010“ hatten mehrere EU-Mitgliedstaaten (Frankreich, Deutschland, Ungarn, Italien, Niederlande, Schweden und Großbritannien) an der dritten zivil-militärischen US-Übung „Cyber Storm“ teilgenommen, die vom Ministerium für Innere Sicherheit der Vereinigten Staaten (DHS) geleitet wurde. Ebenfalls beteiligt waren Australien, Kanada, Japan und Neuseeland. Die Europäische Kommission und ENISA nahmen als Beobachter teil. Das DHS lobte die Übung als einzigartig, da noch mehr Akteure der Privatwirtschaft (60 Firmen) als zuvor beteiligt waren. Am „Cyber Storm III“ arbeiteten das „Department of Defense“, das „Defense Cyber Crime Center“, das „Office of the Joint Chiefs of Staff National Security Agency“, das „United States Cyber Command“ und das „United States Strategic Command“ mit. „Cyber Storm III“ testete das 2009 eröffnete „National Cybersecurity and Communications Integration Center“ (NCCIC).

Verabredet wurde nach Auswertung der „Cyber Storm III“, zukünftig gemeinsame Übungen mit den Mitgliedstaaten der EU abzuhalten. Demnach soll die Kommission 2011 mit den USA in einer neu eingerichteten „high-level EU-US Working Group on cyber security and cybercrime“ (MEMO/10/597) ein „gemeinsames Programm und einen Fahrplan für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013“ entwickeln (Ratsdokument 8548/11). Weitere „Optionen für die Zusammenarbeit mit anderen Regionen oder Ländern“ sollen „erwogen“ werden.

Auf ihrer Sitzung am 14. April 2011 in Gödöllo kamen die Innen- und Justizministerinnen und -minister überein, noch dieses Jahr eine gemeinsame „EU-US cyber-incident exercise“ auszurichten (MEMO/11/246). Wieder sind eine starke Einbindung des „Privatsektors“ und die Beteiligung der „Industrie“ vorgesehen. Szenarien würden demnach eine „Bekämpfung von Botnetzen“ oder die „Verbesserung der Widerstandsfähigkeit und Stabilität des Internets“ sein. Bewusstseinsbildung wie Herangehensweisen sollen demnach vermehrt „über den Atlantik hinweg“ organisiert werden. Anhand von Webseiten mit kinderpornographischem Inhalt soll die EU-/US-Kooperation bei der „Entfernung“ von Webseiten entwickelt werden, darunter auch durch die Arbeit zusammen mit Anbietern von Domainregistrierung. Hierzu gehört ebenso noch 2011 eine Konferenz über „child protection online“ in Silicon Valley.

1. Welche EU-Behörden nehmen mit welchem Personal an der 2010 gegründeten „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ (High-level EU-US Working Group on cyber security and cybercrime) teil?

Die Europäische Union (EU) beteiligt sich an der Arbeitsgruppe mit den zuständigen Behörden und Abteilungen aus den Bereichen Innere Sicherheit, Informationstechnik sowie Strafverfolgung.

a) Welche ähnlichen bilateralen Gespräche oder Initiativen finden zwischen der EU und welchen anderen Regierungen hierzu statt?

Der Bundesregierung ist nicht bekannt, ob die Europäische Kommission neben den Vereinigten Staaten von Amerika (USA) Gespräche mit weiteren bilateralen Partnern zu den Themen Cybersicherheit/Cyberkriminalität führt.

b) Welche „neuen Bedrohungen“ soll die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ konkret adressieren?

Die Arbeitsgruppe wird sich mit IT-Bedrohungen befassen. Mit der Betonung der „neuen“ Bedrohungen soll auf die sich ständig ändernde Cyberbedrohungslage hingewiesen werden.

c) Welche deutschen Behörden sind mit welchem Personal in der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ organisiert?

Themenbezogen sollen sich unterschiedliche Mitarbeiter des Bundesministeriums des Innern (BMI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an der Arbeitsgruppe beteiligen.

d) Welche Ministerien, Behörden oder sonstigen Institutionen sind seitens der USA an der Arbeitsgruppe beteiligt?

Die USA beteiligen sich nach hiesiger Kenntnis an der Arbeitsgruppe mit den zuständigen Behörden und Abteilungen aus den Bereichen Innere Sicherheit, Informationstechnik (BSI) sowie Strafverfolgung.

e) Welche Zusammenarbeit mit anderen Regionen oder Ländern wurde bislang erwogen bzw. verabredet?

Die Bundesregierung hat diesbezüglich keine Vorschläge an die EU herangetragen.

f) Welche Sitzungen der „high-level EU-US Working Group on cyber security and cybercrime“ haben seit ihrer Gründung mit welcher Tagesordnung stattgefunden?

Die „high-level EU-US Working Group on cyber security and cybercrime“ hat nach hiesigem Kenntnisstand bislang noch nicht getagt.

g) Welche Plenartagungen oder Unterarbeitsgruppen werden innerhalb der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ organisiert?

Es wurden vier Unterarbeitsgruppen gebildet:

- „Cyber Incident Management“ mit dem Ziel gemeinsamer Übungen,
- „Public-Private Partnerships“, derzeit mit dem Hauptthema Botnetzbekämpfung,
- „Awareness Raising“, derzeit Informations- und Erfahrungsaustausch,
- „Cyber Crime“.

h) Welche Inhalte eines „Fahrplans für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013“ hat die Arbeitsgruppe bereits entwickelt?

Konkret ist bisher nur eine erste Übung geplant, die im November 2011 stattfinden wird; weitere sollen jedoch grundsätzlich folgen.

i) Innerhalb welcher Treffen hat sich die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ seit ihrem Bestehen auch mit dem Thema „Bekämpfung von kriminellen Inhalten auf Webseiten“ oder „Kinderpornographie“ beschäftigt, und mit welchem Inhalt bzw. Ergebnis?

Die Unterarbeitsgruppe Cybercrime der in der Frage angeführten Arbeitsgruppe hat sich auf einem Treffen am 28./29. Juni 2011 in Brüssel der Thematik „Bekämpfung der Kinderpornografie im Internet“ angenommen. Schwerpunkt war die Erarbeitung von Handlungsleitlinien zur Entfernung von kinderpornografischen Internetinhalten. In diesem Zusammenhang wurde festgestellt, dass das „notice and take down“-Verfahren zwischen europäischen und amerikanischen Stellen in der jüngeren Vergangenheit eine deutliche Verbesserung erfahren habe. Es ist angedacht, die aus dem Informationsaustausch während des Treffens abzuleitenden Handlungsleitlinien bei dem nächsten EU-US-Gipfeltreffen im November 2011 zu behandeln. Ein entsprechender Formulierungsvorschlag liegt der Bundesregierung jedoch noch nicht vor.

2. Welche Tagesordnungspunkte wurden auf dem jüngsten „EU-/US-Senior-Officials-Treffen“ behandelt, und wie wurde dort das Thema „Cyberkriminalität“ adressiert?

Auf der Tagesordnung standen die Themen Cybersicherheit und Cyberkriminalität, Terrorismusbekämpfung und Sicherheit, PNR, Mobilität, Grenzen und Migration, Datenschutz, justizielle Zusammenarbeit in Strafsachen sowie internationale Zusammenarbeit. Im Zusammenhang mit dem Thema Cyberkriminalität betonten beide Seiten die Bedeutung der Zusammenarbeit mit dem privaten Sektor, um die dortigen Fähigkeiten und Kenntnisse zu nutzen. Die USA forderten die EU-Staaten, die das Übereinkommen des Europarats über Zusammenarbeit bei der Bekämpfung der Computerkriminalität vom 23. November 2011 (Budapester Konvention) noch nicht ratifiziert haben, auf, dies umzusetzen. Zu den Einzelheiten wird auf das Ratsdokument „Summary of conclusions of the EU-US JHA Informal Senior Officials Meeting, Cracow, 25-26 July 2011“ (13228/11) verwiesen.

a) Welche Diskussionen wurden hinsichtlich eines „IP-Adressenmissbrauchs“ geführt, und wie ist die Haltung der Bundesregierung hierzu?

Die Problematik einer möglicherweise erhöhten Missbrauchsgefahr von Domainnamen bei der seitens ICANN geplanten Erweiterung der Top-Level-Domains und beim Übergang zu IPv6-Adressen wurde erörtert. ICANN wurde seitens des Rates erneut gebeten, die Vorschläge im Strafverfolgungsbereich zur Minderung der Missbrauchsgefahren umzusetzen. Die Bundesregierung unterstützt dies.

b) Welche Diskussionen wurden hinsichtlich der Bekämpfung von Kinderpornographie geführt, und wie ist die Haltung der Bundesregierung hierzu?

Die Löschung kinderpornographischer Internetinhalte konnte durch intensivere Zusammenarbeit der zuständigen Stellen verbessert werden; mit Blick auf die Bedeutung dieses Themas wird sich die Bundesregierung auch zukünftig um nachhaltige Lösungen bemühen. Wie bereits zu Frage 1 ausgeführt, hat die Unterarbeitsgruppe „Cybercrime“ das Thema aufgegriffen.

c) Welche Verabredungen wurden auf dem „EU-/US-Senior-Officials-Treffen“ getroffen, und welche weiteren Treffen sind 2011 vorgesehen?

Es wurde verabredet, die Themen Cybersicherheit und Cyberkriminalität in verschiedenen Untergruppen weiterzubearbeiten. Beim EU-US-Treffen der Innen- und Justizminister am 2. November 2011 soll Bilanz der bisherigen Aktivitäten zu Cybersicherheit und Cyberkriminalität gezogen und über das weitere Vorgehen gesprochen werden.

3. Welche Regierungen von EU-Mitgliedstaaten sowie anderer Länder waren an der „Cyberstorm III“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?

Deutschland war an einem von der eigentlichen US-Übung getrennten, eigenständigen Strang von Cyber Storm III beteiligt. Übende Nationen (Full-Player) waren hier neben Deutschland auch Frankreich, Japan, die Niederlande, Schweden, Schweiz, Ungarn und die USA (Teile des US-CERT). In einer Beobachterrolle waren Australien, Italien, Kanada, Neuseeland und das Vereinigte Königreich beteiligt. Der Bundesregierung liegen nur Informationen zu dieser Teilübung vor.

a) Welche US-Ministerien bzw. -Behörden waren an „Cyberstorm III“ beteiligt?

An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, nahmen für die USA nur das Department of Homeland Security mit dem US-CERT teil.

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

An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, nahmen nur staatliche Akteure teil.

c) Welche privaten Firmen bzw. sonstigen zivilgesellschaftlichen Akteure haben an „Cyberstorm III“ teilgenommen?

An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, haben keine privaten Firmen bzw. sonstige zivilgesellschaftlichen Akteure teilgenommen.

d) Wie bewertet die Bundesregierung die starke militärische Beteiligung bei der „Cyberstorm III“?

An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, haben keine militärischen Stellen teilgenommen.

e) Wie war die Übung strukturell angelegt, und welche Szenarien wurden durchgespielt?

Der Strang von Cyber Storm III, an dem Deutschland beteiligt war, war eine dislozierte Stabrahmenübung mit einem „Computerwurm"-Szenario.

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

Im BSI haben 25 Mitarbeiter des BSI und ein Mitarbeiter des Bundeskriminalamts (BKA) geübt. Ein Mitarbeiter des BSI war in der zentralen Übungssteuerung in Den Haag.

g) Wie viele Personen haben insgesamt an der „Cyberstorm III" teilgenommen?

An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, haben ca. 100 Personen teilgenommen.

h) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden?

Für den Strang von Cyber Storm III, an dem Deutschland beteiligt war, sind geschätzte Kosten von ca. 69 000 Euro entstanden. Diese wurden aus dem Etat des BSI bestritten.

4. Welche europäischen Länder waren an der „Cyber Europe 2010" aktiv beteiligt, und welche hatten eine beobachtende Position inne?

Es haben alle EU-Mitgliedstaaten sowie drei EFTA-Staaten (Island, Norwegen, Schweiz) aktiv teilgenommen.

a) Wie war die Übung strukturell angelegt, und welche Aufgabe erfüllte das zentrale Lagezentrum in Athen?

Die Teilnehmer haben von ihren Heimatbehörden aus an der Übung teilgenommen. ENISA hat in ihren Büros in Athen ein Exercise Control Center betrieben, das die Übung gesteuert und beobachtet hat. Jeder teilnehmende Staat hat einen Moderator in das Exercise Control Center entsandt.

b) Welche weiteren „Experten von über 70 Einrichtungen des öffentlichen Bereichs und Behörden aus ganz Europa" waren beteiligt?

In den teilnehmenden Staaten wurden Behörden beteiligt, die an der Bewältigung einer IT-Krise beteiligt wären. Weitere Details liegen der Bundesregierung nicht vor.

c) Wie viele Angehörige welcher deutschen Behörden haben an welchen Standorten an der „Cyber Europe 2010" teilgenommen?

In Deutschland haben fünf Mitarbeiter des BSI (Bonn) und der Bundesnetzagentur (BNetzA Saarbrücken) teilgenommen. Ein BSI-Mitarbeiter hat in Athen teilgenommen.

d) Welche Szenarien wurden für die Übung angenommen und durchgespielt, und was ist unter den in der Pressemitteilung des ENISA vom 10. November 2010 gemeldeten 320 „Sicherheitsinjektionen“ zu verstehen?

Es wurde nur ein Szenario geübt. Dabei wurden (stark vereinfacht) fiktive Ausfälle von Internetverbindungen angenommen, um die Kommunikation der Teilnehmer untereinander anzuregen. Ziel der Übung war nicht die technische Wiederinbetriebnahme der Internetverbindungen, sondern die Kommunikation zwischen den beteiligten Behörden.

Die „Sicherheitsinjektionen“ waren die einzelnen Vorkommnisse (z. B. Verbindungsausfälle) im Laufe der Übung, die an die Teilnehmer kommuniziert wurden.

e) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?

Durch die Teilnahme an der Übung sind geschätzte Kosten von ca. 14 400 Euro entstanden. Diese wurden aus dem Etat der beteiligten Behörden bestritten (ca. 96 Prozent BSI, 4 Prozent BNetzA).

5. Welche Vorbereitungen werden von Behörden der EU-Mitgliedstaaten für die Ausrichtung einer „Cyber Europe 2012“ unternommen?

Es werden die grundsätzlich notwendigen Vorbereitungsbesprechungen für Übungen mit internationaler Beteiligung durchgeführt. Die Mitgliedstaaten haben dazu eine Arbeitsgruppe (zu EU-Übungen allgemein) und eine Planungsgruppe etabliert. Die Planungsgruppe erarbeitet mit Unterstützung eines Beratungsunternehmens die Feinplanung der Übung. Die Übung wird im „Europäischen Forum der Mitgliedstaaten“ und im Forum „Europäische öffentlich-private Partnerschaft für Robustheit“ thematisiert.

a) Welche europäischen sowie nichteuropäischen Akteure werden nach derzeitigem Stand teilnehmen bzw. sind an Vorbereitungen beteiligt?

Die Teilnehmer an der Cyber Europe 2012 sind voraussichtlich ausschließlich Akteure aus EU und EFTA.

b) Welche Rolle spielt der innerhalb der „Cyber Europe 2012“ zu testende „Europäische Mechanismus zur Zusammenarbeit bei Netzstörungen“, und was ist darunter zu verstehen?

Gegenwärtig existiert kein „Europäischer Mechanismus zur Zusammenarbeit bei Netzstörungen“. Zur Verbesserung der vorfallbezogenen europäischen Kommunikation wird ein freiwilliger Mechanismus zur Zusammenarbeit bei grenzüberschreitenden europäischen Cybersicherheitsvorfällen erstellt. Dieser soll im Rahmen der Cyber Europe 2012 getestet werden.

6. Welche Aktivitäten oder Übungen sind im Zusammenhang mit dem „Eurocybex-Projekt“ geplant?

Die Eurocybex-Übung fand am 27. September 2011 statt; das Projekt ist nach der Auswertung der Übung abgeschlossen.

a) Welche Behörden und privaten Akteure welcher EU-Mitgliedstaaten sind in das „EuroCybex-Projekt“ integriert?

An der Übung haben die nationalen CERTs von Österreich, Frankreich, Ungarn und Deutschland teilgenommen. Ein französisches Beratungsunternehmen hat als Auftragnehmer die Durchführung der Übung unterstützt. Privatwirtschaftliche Akteure der kritischen Infrastrukturen waren nicht beteiligt.

b) Welche nichteuropäischen Akteure sind darüber hinaus auf welche Art und Weise beteiligt?

Es waren keine außereuropäischen Akteure beteiligt.

7. Welchen Inhalt hatte die in Budapest ausgetragene Konferenz zu „Cybercrime“ vom 12. bis 13. April 2011?

Schwerpunkt der Konferenz waren Themen im Zusammenhang mit dem zehnjährigen Bestehen der Unterzeichnung der Budapester Konvention. Die Konferenz gliederte sich in zwei Teile. Im Rahmen des ersten Teils erfolgte ein Meinungsaustausch zu der Zusammenarbeit zwischen Strafverfolgungsbehörden einerseits und zwischen Strafverfolgungsbehörden und anderen Institutionen anderseits auf Expertenebene. Der zweite Teil der Konferenz widmete sich neben den bereits angeführten Schwerpunkten auf Expertenebene auch den Aspekten der Verbesserung der Zusammenarbeit zwischen den USA und Europa im Hinblick auf Cybercrime.

a) Welche Ministerien bzw. Behörden welcher Länder haben an der Konferenz teilgenommen?

Es haben die Mitgliedstaaten der Europäischen Union zumeist auf Ebene der jeweiligen Innen- bzw. Justizressorts teilgenommen. Eine vollständige Teilnehmerliste liegt der Bundesregierung nicht vor. Seitens der USA haben das Justizministerium und das Department of Homeland Security teilgenommen. Seitens der Europäischen Union haben Vertreter von EUROPOL, von ENISA, des Rates, der Kommission und des Parlamentes teilgenommen.

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

Neben dem Delegationsleiter, dem Parlamentarischen Staatssekretär im Bundesministerium des Innern, Dr. Ole Schröder, waren Vertreter des BMI und des BKA beteiligt.

c) Welche Vertreter welcher US-Behörden haben mit welchem Anliegen an der Konferenz teilgenommen?

Die Konferenz diente dem Informationsaustausch über Möglichkeiten zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden untereinander und Strafverfolgungsbehörden mit privaten Institutionen.

Vertreter der USA brachten ebenso wie Vertreter der Mitgliedstaaten und der EU-Institutionen zum Ausdruck, dass sie an einer engen Kooperation aller im Bereich Cybercrime tätigen Behörden und Institutionen interessiert seien.

d) Welche weiteren privaten Akteure waren auf besagter Konferenz präsent?

Es nahmen Vertreter von CF LABS, Harm Reduction and Public Affairs CEOP, Child Exploitation and Onlinie Protection Centre, Österreichisches Institut für angewandte Telekommunikation, INSAFE, INHOPE, Internet Plus Hungary, Board of Trustees, National Cybersecurity Center Hungary, Hungarian Association of Content Industry und eco Verband der deutschen Internetwirtschaft e. V. teil.

e) Welche konkreten Verabredungen wurden im Rahmen der auf der Konferenz erörterten „Vertiefung der praktischen Zusammenarbeit der Strafverfolgungsbehörden“ getroffen?

Der Bundesregierung sind keine konkreten Verabredungen im Rahmen der Konferenz bekannt. Die Präsidentschaft hat im Nachgang zu der Konferenz ihre Schlussfolgerungen dargelegt (siehe EU-Präsidentschaftsdokument „Results of the conference on cybercrime held on 12-13 April 2011 in Budapest“, 9619/11).

8. Welche weiteren Erläuterungen hat die frühere ungarische Ratspräsidentschaft bezüglich ihres im April 2011 in der Ratsarbeitsgruppe Strafverfolgung vorgebrachten Vorschlags eines „single secure European cyberspace“ gemacht, und falls diese nicht vorgelegt wurden, mit welchem Fortgang der Initiative rechnet die Bundesregierung?

Der ungarische Vorschlag eines „Single secure European cyberspace“ wurde im Rahmen eines Vortrages auf dem Expertentreffen am 12. April 2011 vorgestellt und nicht weiter diskutiert. Das Thema fand in das Ministertreffen keinen Eingang. Die Bundesregierung hat keine Kenntnis, dass diese Initiative derzeit weiterverfolgt wird.

9. Welche Haltung vertritt die Bundesregierung in den Verhandlungen um die Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme bezüglich des Strafmaßes für die von dem Vorschlag erfassten Grundtatbestände, die erschwerenden Umstände und die Vorschriften für die gerichtliche Zuständigkeit?

Nach der vom Rat der Europäischen Union am 9. Juni 2011 beschlossenen gemeinsamen Ausrichtung wird Artikel 11 des Richtlinienvorschlags („Erschwerende Umstände“) gestrichen und teilweise in Artikel 10 („Strafrahmen“) überführt. Aus den Regelungen zum Strafrahmen (Artikel 10) sowie den dorthin überführten Regelungen zu den erschwerenden Umständen ergibt sich kein Änderungsbedarf für das nationale Recht. Ebenso verhält es sich mit den Vorschriften zur gerichtlichen Zuständigkeit (Artikel 13). Dies trägt den Anliegen der Bundesregierung Rechnung.

a) Der Besitz oder Betrieb welcher „Vorrichtungen“ soll nach gegenwärtigem Stand in der Richtlinie kriminalisiert werden?

Nach der vom Rat der Europäischen Union am 9. Juni 2011 beschlossenen gemeinsamen Ausrichtung ist eine Strafbarkeit des Besitzes oder Betriebes von „Vorrichtungen“ nicht mehr vorgesehen.

b) Wie sind bislang „minderschwere Fälle“ definiert?

Ein „minderschwerer Fall“ ist in dem Richtlinienentwurf nicht vorgesehen. Der Richtlinienvorschlag sieht allerdings bei einigen Tatbeständen vor, dass diese

von den Mitgliedstaaten nur unter Strafe zu stellen sind, wenn „kein leichter Fall vorliegt“. Eine Definition enthält der Richtlinienvorschlag nicht.

c) Welche Position vertritt die Bundesregierung hinsichtlich einer „Anstiftung zu Cybercriminalität“, und wie ist diese in der deutschen Strafprozessordnung geregelt?

Die Anstiftung zu Straftaten der Computerkriminalität ist, wie auch für alle übrigen Straftatbestände des Strafgesetzbuches (StGB), im Allgemeinen Teil des StGB (§ 26 StGB) geregelt. Der Richtlinienvorschlag sieht keine darüber hinausgehenden Regelungen vor.

d) Welche Position vertritt die Bundesregierung hinsichtlich eines „Internet Kill Switch“?

Die Bundesregierung lehnt einen sog. Kill Switch für das Internet, also das Zwangsabschalten des gesamten Internets, ab. Ein „Internet-Kill-Switch“ widerspräche der Bedeutung des Internets als grundlegender Infrastruktur und freiheitlichem Kommunikationsmittel.

10. Welche Behörden, privaten Akteure oder sonstigen Institutionen haben in Deutschland CERT aufgebaut, und welche konkreten Ziele und Zwecke werden damit jeweils verfolgt?

Auf Bundesebene verfügen das BSI und die Bundeswehr über ein eigenes CERT.

In Deutschland gibt es ca. 30 CERTs, die sich im deutschen CERT-Verbund organisiert haben (www.cert-verbund.de/). Des Weiteren gibt es geschätzte 250 Teams oder Personen mit ähnlichen Aufgaben. Das Ziel aller ist der verbesserte IT-Schutz der jeweiligen Zielgruppe. Die Aufgaben von CERTs sind jeweils abhängig von der Übertragung im jeweiligen Zielgruppenkontext. In der Regel sind dies:

- Lösung von konkreten IT-Sicherheitsvorfällen, ggf. Koordinierung;
- Warnungen vor Sicherheitslücken und Anbieten von Lösungen.

In Einzelfällen kommen Aufgaben wie IT-Revision, Vor-Ort-Teams, Penetrationstests, Produktunterstützung etc. dazu.

11. Welche EU-Mitgliedstaaten haben der Bundesregierung nationale bzw. private CERT gemeldet, bzw. mit welchen weiteren ausländischen CERT arbeiten deutsche Behörden zusammen?

Welche weiteren CERT sind für weitere EU-Institutionen bis 2012 vorgeschlagen, und wie sind sie bislang umgesetzt?

Es besteht keine Meldepflicht für EU-Mitgliedstaaten gegenüber der Bundesregierung. Grundsätzlich arbeitet das BSI mit allen CERTs weltweit anlassbezogen zusammen. Dies sind mindestens die in der internationalen CERT-Organisation FIRST aufgelisteten Organisationen (www.first.org/members/teams/).

Derzeit ist das EU-Institutionen-CERT im Aufbau, das EU-behördenübergreifend koordinieren soll (http://cert.europa.eu). Der Bundesregierung liegen keine Informationen zu weiteren vorgeschlagenen CERTs bei EU-Institutionen vor.

12. Welche Absicht wird mit den „Operational Action Plans“ (OAP) verfolgt, die innerhalb des von der früheren belgischen Ratspräsidentschaft begonnenen „Policy Cycle“ eingerichtet wurden?

    a) Welche Inhalte sollen in den zukünftigen OAP „Cyberkriminalität“ behandelt werden, und welche Initiativen wären vermutlich damit verbunden?

Am Prioritätsfeld „Cybercrime“ auf EU-Ebene beteiligt sich Deutschland derzeit nicht.

    b) Wie kam die Entscheidung zustande, der rumänischen Delegation die Federführung der OAP zu überlassen, bzw. welche Ausführungen hatte diese zuvor dazu gemacht?

Für jedes Prioritätsfeld wird ein federführender Mitgliedstaat bestimmt. Für „Cybercrime“ wird Rumänien diese Rolle übernehmen. Näheres ist hier nicht bekannt.

    c) Wie ist die Polizeiagentur Europol in die Umsetzung der OAP eingebunden?

Europol ist im Rahmen seiner ihm übertragenen Aufgaben eingebunden. Europol wird zusammen mit der polnischen Ratspräsidentschaft Gastgeber des Workshops zur Erarbeitung der „Operational Action Plans“ sein.

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

    Welche EU-Mitgliedstaaten bzw. anderen Regierungen wurden 2010 und 2011 von der ENISA unterstützt, nationale Notfallpläne aufzustellen oder Übungen durchzuführen?

Im EU-Parlament befindet sich die Mandatierung noch in erster Lesung. Über den zuständigen Ausschuss (Committee on Industry, Research and Energy, ITRE) wurde ein Draft-Report (sog. Chichester-Report) mit Vorschlägen zur Mandatserweiterung veröffentlicht. Nach Kenntnis der Bundesregierung hat der Ausschuss diesen Bericht jedoch noch nicht verabschiedet und noch keine formale Stellungnahme abgegeben.

Im Rat wird die Mandatierung seit November 2010 verhandelt – die ungarische Präsidentschaft hatte dem Rat für Telekommunikation im Mai 2011 einen Fortschrittsbericht zur Kenntnis gegeben.

Im Rahmen von Workshops hat ENISA zehn EU-Mitgliedstaaten bei der Planung von nationalen IT-Krisenübungen unterstützt. Nach Kenntnis der Bundesregierung besteht bei einer Reihe weiterer Mitgliedstaaten ebenfalls Interesse/Bedarf nach einer solchen Unterstützung. Um welche Mitgliedstaaten es sich handelt, ist nicht bekannt.

14. Wie beteiligt sich die Bundesregierung am Aufbau eines „Europäischen Informations- und Warnsystems“ (EISAS)?

Deutschland verfolgt den Aufbau im Rahmen seiner EU-Aktivitäten zum Schutz Kritischer Informations-Infrastrukturen (KII).

a) Welche Stellen innerhalb der EU sollen an das EISAS angeschlossen sein?

Gemäß Planung der Europäischen Kommission soll EISAS hauptsächlich durch die nationalen CERTs mit Inhalten beliefert werden.

b) Wen soll das EISAS mit zukünftigen Informationen beliefern?

Zielgruppen von EISAS sind mittelständische Unternehmen und Bürger.

15. Welche Behörden bzw. Abteilungen der Bundesregierung sowie deutschen privaten Akteure sind in der „Europäischen öffentlich-privaten Partnerschaft für Robustheit“ (EP3R) organisiert?

EP3R ist ein öffentliches Forum. Von deutscher Seite nehmen BSI und BNetzA teil.

Private Akteure sind deutsche Unternehmen und Verbände aus dem IKT-Sektor.

a) Was ist unter den dort formulierten „Zielen für Sicherheit und Robustheit“ sowie „bewährten Maßnahmen“ zu verstehen?

Generell soll die Sicherheit (d. h. die Vertraulichkeit, Verfügbarkeit und Integrität) von IKT-Infrastrukturen gefördert werden. Unter „Sicherheit“ wird oftmals nur der Schutz von vertraulichen Daten verstanden, weshalb zusätzlich die Bedeutung der Verfügbarkeit/Robustheit von kritischen IKT-Dienstleistungen herausgehoben wird.

b) Mit welchen „Partnern aus Drittländern“ bzw. welchen ihrer Behörden oder privaten Akteuren wird innerhalb der EP3R zusammengearbeitet?

Derzeit gibt es im EP3R noch keine etablierte Zusammenarbeit mit Ländern außerhalb der EU.

c) Wie ist die ENISA in den Aufbau bzw. die Tätigkeit der EP3R eingebunden?

ENISA unterstützt die Prozesse des EP3R. ENISA führt Sitzungen durch, betreibt ein Portal für den internen Informationsaustausch, erstellt Dokumente für die Sitzungen und berichtet über die ENISA-Aktivitäten im Themenkontext.

d) Nach welchem Verfahren wurden Ziele, Grundsätze und Aufbau der EP3R festgelegt?

Die Einrichtung des EP3R basiert auf dem CIIP Action Plan der Europäischen Kommission von 2009. Im EP3R wurden Arbeitsgruppen gegründet. In diesen Arbeitsgruppen wurden „Terms of reference“ für die jeweilige Arbeitsgruppe erarbeitet.

e) Wie ist die EP3R in die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ eingebunden?

Ergebnisse aus der Arbeitsgruppe EU-USA werden in EP3R kommuniziert.

16. Welche Behörden bzw. Abteilungen der Bundesregierung sowie deutscher privater Akteure sind im „Europäischen Forum der Mitgliedstaaten“ (EFMS) vertreten?

Von deutscher Seite nehmen das BMI, das BSI und die BNetzA teil. Private Akteure sind nicht beteiligt.

a) Auf welche Art und Weise arbeitet das EFMS mit der ENISA zusammen?

ENISA unterstützt die Prozesse des EFMS. ENISA führt Sitzungen durch, betreibt ein Portal für den internen Informationsaustausch, erstellt Dokumente für die Sitzungen und berichtet über die ENISA-Aktivitäten im Themenkontext.

b) Welche Rolle spielt das EFMS bei der Ausgestaltung von Cyber-Übungen?

Das EFMS diskutiert die grobe Ausrichtung von Übungen, wirkt jedoch nicht an der konkreten Ausgestaltung der EU-weiten Übungen mit. Hierzu wurde eine eigene Arbeitsgruppe gegründet (siehe Antwort zu Frage 5).

c) Welche konkreten „technischen Erörterungen“ sind hierfür bislang verfasst worden?

ENISA hat einen Good Practice Guide für Übungen erstellt (siehe www.enisa.europa.eu/act/res/policies/good-practices-1/exercises).

d) Wie ist das EFMS in die internationale Zusammenarbeit integriert?

Derzeit arbeitet das EFMS nur mit der EU-USA-Arbeitsgruppe zusammen.

e) Welche Ziele und Zwecke werden mit der Tätigkeit des EFMS in der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ verfolgt?

In den der EU-USA-Arbeitsgruppe zuarbeitenden Expertengruppen („expert sub group“) sind nicht alle Mitgliedstaaten der EU vertreten. Das EFMS bietet allen Mitgliedstaaten die Möglichkeit, sich über die Aktivitäten der EU-USA-Kooperation zu informieren und daran mitzuwirken.

f) Welche „Bewertung des Grades der Cybersicherheit in Europa“ hat das EFMS 2010 und 2011 analysiert, und wie wurde diese ermittelt?

Dieses Thema wurde im EFMS noch nicht behandelt.

17. Mit welchen „internationalen Partnern“, insbesondere aus den USA, der G8 und der OECD, hat die Europäische Kommission 2011 die „Grundsätze und Leitlinien für die Robustheit und Stabilität des Internets“, wie in der „Mitteilung über den Schutz kritischer Informationsinfrastrukturen – Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit“ vom 31. März 2011 beschrieben, erörtert?

Welche Ergebnisse zeitigte die weitere Erörterung „mit relevanten Akteuren, insbesondere des Privatsektors“, und welche sind hiermit konkret gemeint?

Soweit hier bekannt, wurde das Papier bisher nur in die Zusammenarbeit mit den USA (EU-USA-Arbeitsgruppe) eingebracht; außerdem wurde es im EP3R der Privatwirtschaft vorgestellt.

Reaktionen auf das Papier liegen der Bundesregierung nicht vor.

18. Inwieweit sind welche deutschen Behörden oder privaten Akteure in die in London gestartete „International Cyber Security Protection Alliance“ (ICSPA) eingebunden?

a) Von welchen EU-Institutionen bzw. -Regierungen wird die Initiative finanziert?

b) Mit welchen Arbeitsgruppen und Aufgaben nimmt die EU-Polizeiagentur EUROPOL an der ICSPA teil?

Die Bundesregierung ist an der ICSPA nicht beteiligt. Über eine Beteiligung von Behörden der Länder oder Privater sowie zur Finanzierung der ICSPA liegen der Bundesregierung keine Kenntnisse vor.

19. Welche Erkenntnisse hat die Bundesregierung darüber, wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat?

Der Bundesregierung liegen keine Informationen darüber vor, dass es bisher einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat. Zu den Arbeiten an einer Definition des Phänomens „Cyber-Terrorismus“ vergleiche Antwort zu Frage 22.

a) Würde die Bundesregierung das Auftauchen von „Stuxnet“ als „cyberterroristischen Anschlag“ kategorisieren?

Der Bundesregierung liegen keine belastbaren Erkenntnisse zur konkreten Urheberschaft von „Stuxnet“ vor. Komplexität, Wirkungsweise und Angriffsziel dieses Computervirus lassen auf höchste Professionalität mit den notwendigen personellen und finanziellen Ressourcen schließen, was einen nachrichtendienstlichen Hintergrund des Angriffs nahelegt. Insofern geht die Bundesregierung nach den vorliegenden Erkenntnissen bei „Stuxnet“ nicht von einem cyberterroristischen Anschlag aus.

b) Falls es bislang keine bekannten „cyberterroristischen Anschläge“ gegeben hat, auf welche Annahmen oder wenigstens Risikoanalysen gründen sich die zahlreichen EU-Verlautbarungen und Forderungen (unter anderem des EU-Anti-Terrorismuskoordinators) zur Bekämpfung derselben?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Über welche Studien bzw. Risikoanalysen verfügt die Bundesregierung bezüglich der Wahrscheinlichkeit eines größeren Ausfalls von Informationsinfrastrukturen?

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat einen Bericht zu langandauernden großflächigen Stromausfällen veröffentlicht (Bundestagsdrucksache 17/5672). Hier wird der Ausfall von IKT-Dienstleistungen in einem eigenen Kapitel behandelt.

d) Über welche Studien bzw. Risikoanalysen verfügt die Bundesregierung bezüglich der Wahrscheinlichkeit einer Zerstörung kritischer Infrastruktur durch digitale Angriffe?

Die Bundesregierung verfügt über keine Studien oder Risikoanalysen bezüglich der Wahrscheinlichkeit einer Zerstörung kritischer Infrastruktur durch digitale Angriffe.

20. Welches Szenario liegt der diesjährigen „Länder Übergreifenden Krisenmanagementübung (Xercise)“ (LÜKEX) vom 30. November bis 1. Dezember 2011 zugrunde?

Die LÜKEX 2011 wird sich mit den Herausforderungen befassen, die das gemeinsame Krisenmanagement des Bundes und der Länder bei bewusst herbeigeführten IT-Vorfällen zu bewältigen hätte. So sollen Auswirkungen auf die Bundesverwaltung, die Netze von Bundesländern sowie Betreibern Kritischer Infrastrukturen (z. B. der Verkehrsleitsysteme), die ein komplexes Schadprogramm verursachen könnte, simuliert werden.

a) Welche Krisenstäbe des Bundes und der Länder werden sich hierfür mit welchen Lagezentren beteiligen?

An der LÜKEX 2011 wird sich das BMI mit seinem Krisenstab und Lagezentrum unter Einbeziehung weiterer Behörden des Bundes beteiligen.

Die Länder Hamburg, Niedersachsen, Sachsen, Hessen und Thüringen werden als intensiv übende Länder mit Krisenstäben teilnehmen. Darüber hinaus sind die Länder Berlin, Baden-Württemberg, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen-Anhalt, Bayern und Brandenburg mit einer geringeren Beteiligungstiefe in die Übung eingebunden.

b) Wer ist verantwortlich für das Erstellen bzw. den Inhalt fiktiver TV-Sendungen, Presseberichte und -kommentare sowie Anfragen von Journalisten?

Einer der Schwerpunkte der LÜKEX 2011 ist das Zusammenwirken im Rahmen einer abgestimmten und aktiven Öffentlichkeitsarbeit zur situationsgerechten Information der Bevölkerung.

Dafür wird im Rahmen der LÜKEX 2011 eine fiktive Medienlandschaft u. a. mit „LÜKEX TV“, Printmedien als vereinfachtem Spiegelbild der deutschen Medienlandschaft und ausgewählten internationalen Medien durch das BBK in Abstimmung mit dem BMI erstellt.

c) Inwieweit berücksichtigt die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf Kritische Infrastruktur?

Die Übung hat ein IT-Sicherheitsszenario als Thema. Damit werden auch Angriffe über das Internet auf Kritische Infrastrukturen angenommen. Es werden keine „cyberterroristische Anschläge“ eingespielt.

d) Welche ausländischen privaten oder öffentlichen Stellen sind in die Übung integriert oder beobachten diese?

LÜKEX ist eine nationale Krisenmanagementübung des Bundes und der Bundesländer auf der strategischen Ebene, in die Ministerien, Bundesbehörden, Hilfsorganisationen, Verbände und Wirtschaftsunternehmen einbezogen sind. Wissenschaft und Forschung begleiten und unterstützen die Übung durch fachliche Beratung. Vor diesem Hintergrund ist lediglich eine begrenzte internationale Beteiligung (z. B. Europäischer CERT-Verbund) in der zentralen Übungssteuerung vorgesehen. Internationalen Besuchern wird im Rahmen eines IT-Forums die Gelegenheit zur Information über die Übung eingeräumt.

21. Entspricht die Erklärung vom Ministerialrat und Referatsleiter im Bundesministerium der Verteidigung, Horst Stern, auf der Tagung der Bundesakademie für Sicherheitspolitik „Auf dem Weg zur Automatisierung und Digitalisierung des Krieges?“ am 11. November 2010 „[…] Alle Versuche, eine Gesellschaft, ihren Staat oder ihre wirtschaftlichen Verhältnisse zu ändern sind politisch. Hier ist die Bundeswehr einzusetzen“ der Haltung der Bundesregierung, und falls nein, wie wird sie diese Darstellung korrigieren?

Nach bisherigen Erkenntnissen hat kein Angehöriger des Verteidigungsressorts bei der genannten Veranstaltung eine derartige Äußerung getätigt. Sie entspricht auch nicht der Haltung der Bundesregierung.

22. Wie steht die Bundesregierung zum Vorschlag des polnischen Ratsvorsitzes, einer potentiellen „cyberterroristischen Bedrohung“ auf EU-Ebene mittels Erstellung eines übergreifenden „Glossars“ zu begegnen, innerhalb dessen die Praktiken von Cyberabwehrstrukturen der Mitgliedstaaten evaluiert werden?

Ziel der Erarbeitung eines Glossars ist es, ein gemeinsames Verständnis des Phänomens Cyberterrorismus zu erlangen und einheitliche Definitionen für einschlägige Begriffe festzulegen. Diesem Vorschlag steht die Bundesregierung aufgeschlossen gegenüber; im Rahmen der Anti-Terror-Arbeitsgruppen sollen jedoch Arbeiten insgesamt und auch der Fragebogen auf Terroraspekte der Cyberbedrohungen beschränkt werden.

a) Welche Haltung vertritt der EU-„Anti-Terrorismuskoordinator“ hierzu, und wie begründet er diese in den zuständigen Ratsarbeitsgruppen gegenüber Delegationen der Bundesregierung?

Nach dem Kenntnisstand der Bundesregierung unterstützt der EU-Antiterrorismuskoordinator im Grundsatz die Vorschläge der polnischen Ratspräsidentschaft.

b) Wie bewertet die Bundesregierung die Absicht, im Glossar eine aus NATO-Strategien übernommene Formulierung zur bestehenden Gefahr „cyberterroristischer“ Anschläge aufzunehmen, obschon es bislang weltweit noch keinen bekannten „cyberterroristischen“ Angriff gegeben hat?

Die Bundesregierung hält es für sinnvoll, dass auf EU-Ebene eine einheitliche Definition für das Phänomen Cyberterrorismus erarbeitet wird. Auf die Antwort zu Frage 19 wird verwiesen. Im Übrigen hält die Bundesregierung eine bloße Übernahme der NATO-Terminologie für zivile Zwecke nicht für sinnvoll.

23. Wie ist der Europäische Auswärtige Dienst, der EU-Militärstab (mit seinem „Capability developement plan“) oder die NATO (mit ihrem „Strategic Concept on Cybersecurity“) in die konkrete Ausgestaltung übergreifender Konzepte zur Cybersicherheit in der EU beteiligt?

Für Fragen der Cybersicherheit ist die internationale Zusammenarbeit von erheblicher Bedeutung. Daher kommt auch bei der Entwicklung und Umsetzung übergreifender Konzepte der europäischen Ebene grundsätzlich eine erhebliche Bedeutung zu. Bei der konkreten Ausgestaltung entsprechender Konzepte zur Cybersicherheit in der EU ist die NATO nach Kenntnis der Bundesregierung nicht beteiligt. Zur wachsenden Bedeutung der internationalen Zusammenarbeit wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion

BÜNDNIS 90/DIE GRÜNEN zum Betreff „Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung“, Bundestagsdruckdache 17/6971 vom 18. August 2011, verwiesen.

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