Deutscher Bundestag **Drucksache 17/11757**

17. Wahlperiode 28. 11. 2012

Kleine Anfrage

der Abgeordneten Andrej Hunko, Herbert Behrens, Jan van Aken, Annette Groth, Ulla Jelpke, Niema Movassat, Kathrin Senger-Schäfer, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.

Zusammenarbeit deutscher Behörden bei „grenzüberschreitenden europäischen Cybersicherheitsvorfällen“

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).

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 zusammen-

tragen“. 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.

Wir fragen die Bundesregierung:

1. Auf welche Weise soll das „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ in den operativen Betrieb übergehen?
   a) Welche Aufgabe hat das Zentrum, und wie korrespondiert es mit Strukturen der Bundesregierung, die sich ebenfalls mit „Cybersicherheit“ befassen?
   b) Wo wird das Zentrum angesiedelt, und mit welchen Mitarbeiterinnen und Mitarbeitern wird es nach derzeitiger Planung ausgestattet?
   c) Wie viele der Mitarbeiterinnen und Mitarbeiter gehören zu welchen Abteilungen der Polizeiagentur Europol?
   d) Inwieweit und mit welchen Kapazitäten sind Behörden aus „Drittstaaten“ eingebunden?
   e) Welche internationalen Organisationen, Internetdienstleister oder Interessenverbände sind am „EU-Zentrum zur Bekämpfung der Cyberkriminalität“ beteiligt?
   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?
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)?
   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?
   c) Wie ist die Bundesregierung daran beteiligt?
   d) Was ist damit gemeint, wenn Europol neue „means of modern information processing tools“ entwickelt (Europol Work Programme 2013, Ratsdokument 12667/12)?
3. Inwieweit ist das CERT-EU von einem Pilotprojekt zu einer permanenten Einrichtung geworden (heise.de, 12. September 2012)?
   a) Mit welcher Aufgabenstellung wurde das CERT-EU errichtet?
   b) Über wie viele Mitarbeiterinnen und Mitarbeiter verfügt das CERT-EU, und wo ist es angesiedelt?
   c) Inwieweit ist das CERT-EU auch mit der Vorbeugung oder Bekämpfung speziell politisch motivierter Proteste von Gruppen wie „Anonymous“ befasst?

4. Auf welche Weise sind Regierungen von EU-Mitgliedstaaten im CERT-EU vertreten?
   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?
   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?
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?
   b) Welche besonderen Bedrohungen haben Bundesbehörden hierfür analysiert, und was wurde der Europäischen Kommission dazu mitgeteilt?
6. Welche „Angriffe“ auf Computer bzw. Computersysteme von Angehörigen des Rates der Europäischen Union wurden in den Jahren 2011 und 2012 jeweils verzeichnet?
   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?
7. Welche „Angriffe“ auf Computer bzw. Computersysteme von Institutionen der Bundesregierung wurden in den Jahren 2011 und 2012 jeweils verzeichnet?
   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)?
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)?
   a) Auf welche Weise wurde dieser bzw. ein vergleichbarer „Mechanismus“ entwickelt, und wer war daran beteiligt?
   b) Auf welche Weise wurde dieser bzw. ein vergleichbarer „Mechanismus“ bei der diesjährigen Übung getestet?
9. Welche Konferenzen zu „Cybersicherheit“ haben auf Ebene der Europäischen Union in den Jahren 2011 und 2012 stattgefunden?
   a) Welche Tagesordnung bzw. Zielsetzung hatten diese jeweils?
   b) Wer hat diese jeweils organisiert und vorbereitet?
   c) Welche weiteren Nicht-EU-Staaten waren daran mit welcher Zielsetzung beteiligt?

d) Mit welchen Aufgaben oder Beiträgen waren auch Behörden der USA eingebunden?

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

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

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?

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?

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

a) Welche Aufgabe übernehmen private Firmen in der ECTEG?

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

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

a) Welche Aufgabe übernehmen private Firmen in der EUCTF?

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

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?

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

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

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

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

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?

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

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

    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?

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?

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?

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?

    a) Welche Arbeitsgruppe oder Unterarbeitsgruppen existieren innerhalb des EP3R?

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

    c) Wer hat die Treffen jeweils vorbereitet?

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

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

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

    a) Welche Arbeitsgruppe oder Unterarbeitsgruppen existieren innerhalb des EFMS?

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

    c) Wer hat die Treffen jeweils vorbereitet?

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

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

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

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

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

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

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

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

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

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

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

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

d) Welche Beispiele existieren, um diese zu begrenzen?

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

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)?

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

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)?

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?

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

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

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?

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)?

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

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

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)?

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?

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)?

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

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

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

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)?

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)?

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?

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?

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?

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?

Berlin, den 28. November 2012

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333