Deutscher Bundestag **Drucksache 19/2618**

19. Wahlperiode 08.06.2018

Kleine Anfrage

der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, Dr. Tobias Lindner, Tabea Rößner, Katja Keul, Dr. Anna Christmann, Dieter Janecek, Dr. Danyal Bayaz, Beate Müller-Gemmeke, Stefan Gelbhaar, Ingrid Nestle, Dr. Konstantin von Notz, Katja Dörner, Maria Klein-Schmeink, Margit Stumpp, Cem Özdemir, Margarete Bause, Dr. Franziska Brantner, Kai Gehring, Uwe Kekeritz, Omid Nouripour, Claudia Roth (Augsburg), Manuel Sarrazin, Dr. Frithjof Schmidt, Jürgen Trittin, Ottmar von Holtz, Irene Mihalic und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Aktivitäten der Bundeswehr im digitalen Raum und gesetzgeberische Maßnahmen der Bundesregierung

Im April 2017 wurde das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr aufgestellt. In diesem Kommando wurden bereits vorhandene und neue IT-Strukturen der Bundeswehr gebündelt. Mit diesem strukturell-organisatorischen Schritt will die Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, auf die sicherheitspolitischen Herausforderungen im digitalen Raum reagieren. Auch ein Jahr nach der Aufstellung des KdoCIR sind zentrale Fragen im Zusammenhang mit dem Aufbau, den rechtlichen Grundlagen, dem Vorhalten und der potenziellen Anwendung von digitalen Einsatzfähigkeiten der Bundeswehr unbeantwortet.

Die Bundeswehr muss sich auf die sicherheitspolitischen Herausforderungen im digitalen Raum und damit verbundene neue Bedrohungslagen einstellen. Zwingend notwendig sind ein verbesserter Eigenschutz und die Härtung der IT-Infrastrukturen der Bundeswehr. Dieser verbesserte Schutz muss sowohl der Sicherung der eigenen Systeme im Rahmen der Landes- und Bündnisverteidigung als auch dem Schutz von Soldatinnen und Soldaten sowie Auslandseinsätzen der Bundeswehr dienen.

Anstatt sich jedoch auf den wichtigen Schutz der eigenen IT-Infrastruktur zu konzentrieren, hatte Bundesverteidigungsministerin Dr. Ursula von der Leyen bereits im Weißbuch 2016 angekündigt, die Bundeswehr offensive Fähigkeiten nicht nur üben und entwickeln zu lassen. Auch der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, spricht in einem Interview von der Notwendigkeit, „Angriffe auch offensiv abwehren zu können“ (www.handelsblatt.com/politik/deutschland/cyber-general-ludwig-leinhos-die-bedrohung-aus-dem-netz-ist-real-und-sie-wird-zunehmen/21182502.html).

Im September 2016 berichtete „SPIEGEL ONLINE“ über eine im Herbst 2015 erfolgte Operation der damaligen Einheit „Computer Netzwerk Operationen“ (CNO), bei der in das System eines afghanischen Mobilfunkbetreibers eingedrungen wurde (vgl.: www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html).

Ein solches Vorgehen birgt aus Sicht der Fragesteller erhebliche Gefahren und gefährdet zudem die Entwicklung eines freien und sicheren Internets. Es stellen sich zahlreiche rechtliche und verfassungsrechtliche Fragen, die bis heute nicht ausreichend beantwortet sind. Der fortwährende Verweis auf die Besonderheiten des Cyber- und Informationsraums und die daraus resultierenden speziellen sicherheitspolitischen Herausforderungen, wie der oftmals fehlende oder unklare rechtliche Rahmen oder der Bedeutungsverlust nationaler Grenzen im digitalen Raum, entbindet die Bundesregierung nicht davon, die notwendigen rechtlichen Grundlagen für ein verfassungsgemäßes Handeln der Bundeswehr zu schaffen.

Dies gilt auch und besonders für die parlamentarische Kontrolle durch den Deutschen Bundestag beim Einsatz von digitalen Einsatzkapazitäten der Bundeswehr, analog zu den bereits bestehenden Regeln beim Einsatz militärischer Kräfte. Für eine effektive demokratische Kontrolle der Parlamentsarmee ist es aus Sicht der Fragesteller unerlässlich, dass der Deutsche Bundestag in Zukunft über die konkreten Details von Operationen der Bundeswehr im digitalen Raum besser und transparenter informiert wird. Nur so kann eine wirksame parlamentarische Kontrolle der Aktivitäten der Bundeswehr im digitalen Raum gewährleistet werden.

Während die weltweite Zahl an IT-Angriffen kontinuierlich steigt und zivile und staatliche digitale Infrastrukturen immer wieder attackiert werden, gibt es derzeit keine wirklichen Fortschritte bei der Erarbeitung konkreter internationaler Vereinbarungen zum Schutz digitaler Infrastrukturen und zur Gewährleistung einer effektiven IT-Sicherheit im Netz. Es reicht nicht, lediglich festzustellen, dass die Prozesse mit Blick auf international verbindliche Regelwerke oder vertrauens- und sicherheitsbildende Maßnahmen höchst schleppend vorangehen und wenig konkrete Ergebnisse erzielen konnten. Stattdessen sollte sich die Bundesregierung auf internationaler Ebene beispielsweise entschieden für einen Verhaltenskodex einsetzen, der u. a. eine Selbstverpflichtung enthält, zivile (Netz-)Infrastruktur nicht für militärische Angriffe durch digitale Angriffskapazitäten zu nutzen oder selbst zum Angriffsziel zu machen.

Wir fragen die Bundesregierung:

1. Wie definiert die Bundesregierung einen „Cyber-Angriff“?

   Nach welchen Kategorien erfolgt eine solche Klassifizierung?

   Welche Standards hat die Bundesregierung für Reaktionen auf solche Angriffe festgelegt, und bei welchen Stellen liegt die diesbezügliche Entscheidungsgewalt?

2. Auf welcher Ebene wird innerhalb der Bundesregierung aufgrund von welchen Rechtsgrundlagen entschieden, welche Stellen mit welcher Maßnahme auf eine Bedrohung oder einen Angriff auf die IT-Infrastruktur reagieren oder ob gar in fremde Netze gewirkt wird?

   Wie sieht hier die Aufgabenteilung insbesondere zwischen dem Bundesministerium des Innern, für Bau und Heimat und seinen Stellen bzw. Behörden, dem Bundesministerium der Verteidigung und seinen Stellen und den Nachrichtendiensten aus?

3. Wie viele IT-Angriffe gab es jeweils in den letzten fünf Jahren und bisher im Jahr 2018 auf die Bundeswehr im Inland?

   a) Wie viele der IT-Angriffe sind als zielgerichtete Attacken auf die Systeme der Bundeswehr einzustufen?

   b) Bei wie vielen dieser Angriffe ist ein Angreifer tatsächlich in Rechner oder Netzwerke der Bundeswehr eingedrungen?

      Wie viele dieser Angriffe beinhalteten gezieltes Kontaktieren oder Ausspionieren von Bundeswehrangehörigen, sogenanntes Social Engineering?

   c) Wie viele Angriffe konnten jeweils in den letzten fünf Jahren und im Jahr 2018 bereits durch übliche Schutzeinrichtungen wie Firewalls etc. abgewehrt werden?

   d) Welche Schäden wurden durch diese IT-Angriffe tatsächlich jeweils bewirkt?

4. Wie viele der bis 2022 geplanten 15 000 Stellen des Kommandos Cyber- und Informationsraumes (KdoCIR) sind bis zum gegenwärtigen Zeitpunkt tatsächlich bereits besetzt?

   Wie viele der derzeit vorgesehenen Dienstposten im KdoCIR sind aktuell aus welchen Gründen nicht besetzt?

5. Wie weit ist der Aufbau einer „Cyber-Reserve“ fortgeschritten?

   Wie viele Dienstposten für Reservistinnen und Reservisten sind für die „Cyber-Reserve“ eingeplant, und wie viele dieser Posten sind aktuell tatsächlich bereits besetzt?

6. Welche konkreten Fähigkeiten meint die Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, wenn sie, wie auf der Bundeswehrtagung am 14. Mai 2018, davon spricht, dass man für die Bundeswehr ein „volles Fähigkeitenspektrum im Bereich Cybersicherheit“ wolle?

7. Welche konkreten Fähigkeiten meint nach Ansicht der Bundesregierung der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, wenn er von benötigten Optionen für die offensive Abwehr von IT-Angriffen spricht (Quelle siehe Vorbemerkung der Fragesteller)?

   Sind hierunter auch aktive Angriffe auf fremde Server („Hackback“) zu verstehen?

8. Wie definiert die Bundesregierung einen „Hackback“, und auf welche Szenarien bezieht sie sich, wenn von einem solchen die Rede ist?

   Welche konkreten Fähigkeiten für „Hackbacks“ will die Bundesregierung in welchen Sicherheitsbehörden oder der Bundeswehr ansiedeln (vgl. beispielhaft die Äußerung vom Präsident des Bundesamts für Verfassungsschutz Hans Georg Maaßen im ARD-Interview, www.tagesschau.de/inland/maassen-cyberangriffe-103.html)?

9. Wie bewertet die Bundesregierung die Frage nach der Verfassungskonformität von aktiven Angriffen auf fremde Server („Hackback“) durch die Bundeswehr?

10. Teilt die Bundesregierung die Ansicht der Fragestellenden, dass es für aktive Angriffe auf fremde Server („Hackback“) heute keine ausreichende Rechtsgrundlage gibt?

11. Plant die Bundesregierung die Schaffung einer Rechtsgrundlage für aktive Angriffe auf fremde Server („Hackback“)?

    Falls ja, bis wann soll eine solche erarbeitet werden?

12. Ist die Bundesregierung der Ansicht, dass ein aktiver Angriff auf fremde Server („Hackback“) durch die Bundeswehr vom Deutschen Bundestag mandatiert werden muss, und wenn nein, warum nicht?

13. Wie beurteilt die Bundesregierung im Kontext der vorausgegangenen Fragen die Attributions-Problematik bei IT-Angriffen und ihrer Abwehr?

14. Wie will man gegebenenfalls verhindern, dass bei einem „Hackback“ und anderen Maßnahmen auch zivile Infrastrukturen in Mitleidenschaft gezogen werden?

    Welche Schutzmechanismen sind hier aus Sicht der Bundesregierung denkbar und notwendig, und wie sind diese in der Praxis umsetzbar?

15. Wie bewertet die Bundesregierung das Risiko, dass eine präventive Infiltrierung bzw. Kompromittierung von fremden Servern (welche in bestimmten Szenarien eine technische Voraussetzung für einen „Hackback“ darstellen kann) ihrerseits von ausländischen Streitkräften oder Geheimdiensten als offensiver Akt gewertet werden könnte?

16. Welche Reaktionsszenarien auf IT-Angriffe werden durch welche Einheiten des Kommandos Cyber- und Informationsraum (KdoCIR) geübt?

17. Welche konkreten Fortschritte wurden seit der Aufstellung des KdoCIR in der Härtung der Infrastruktur und der Systeme der Bundeswehr gemacht?

18. Wie ist der Umgang mit Sicherheitslücken in fremden oder eigenen Systemen, die durch die Bundeswehr im Rahmen von Operationen und Übungen national wie international entdeckt werden?

    Werden entdeckte Sicherheitslücken gemeldet?

    Wenn ja, an wen, und wie oft kam das bisher vor (bitte konkret aufschlüsseln)?

    Wenn nein, warum nicht?

19. Plant die Bundesregierung eine gesetzliche Regelung zur Schaffung einer Meldepflicht von Sicherheitslücken durch staatliche Stellen?

    Falls ja, wie soll diese konkret ausgestaltet sein?

    Falls nein, warum nicht?

20. Inwieweit hält es die Bundesregierung für rechtlich zulässig, sogenannte Zero-Day-Lücken zu erwerben, um sie gegebenenfalls selbst zu nutzen?

    Hat die Bundesregierung Kenntnis davon, ob so ein Erwerb durch staatliche Organisationen oder Behörden bereits stattgefunden hat oder geplant ist (bitte detailliert und einzeln aufführen)?

    Wenn ja, unter welchen Rahmenbedingungen und zu welchem Zweck hält die Bundesregierung ein solches Vorgehen für legitim, erforderlich und rechtskonform?

21. Teilt die Bundesregierung die Auffassung der Fragestellenden, dass Sicherheitslücken, die nicht schnellstmöglich geschlossen werden, immer auch Dritten offenstehen, die diese für IT-Angriffe nutzen können, wodurch sich signifikante Probleme für die IT-Sicherheit insgesamt ergeben?

22. Wie viele Schwachstellen in Netzwerken von Dienststellen der Bundeswehr konnten bisher durch Angehörige des KdoCIR aufgedeckt und geschlossen werden?

    Wie viele dieser entdeckten Schwachstellen wurden im Rahmen von Übungen bzw. während der Abwehr von tatsächlichen IT-Angriffen entdeckt?

23. Welche konkreten Regelungen und datenschutzrechtlichen Bestimmungen kommen nach Auffassung der Bundesregierung für die Verarbeitung aller Verfahren und Prozesse der Bundeswehr, insbesondere auch im Rahmen von Cybersicherheitsaktivitäten, zur Anwendung (bitte im Einzelnen auflisten)?

24. Inwiefern analysiert die Bundeswehr im Rahmen von Übungen die möglichen Auswirkungen auf Zivilistinnen und Zivilisten und zivile Infrastruktur von Operationen im digitalen Raum?

    a) Ist diese Analyseperspektive festintegrierter Bestandteil jedes Übungsszenarios?

       Wenn nein, warum nicht?

    b) Durch welche konkreten Mechanismen wird sichergestellt, dass das Unterscheidungsgebot zwischen Kombattantinnen und Kombattanten und der Zivilbevölkerung bei Operationen im digitalen Raum (im konkreten Einsatz- und im Übungsfall) stets beachtet wird?

25. Wie hoch waren 2017 und 2018 die Kosten für die speziell auf eine Nachwuchsgewinnung für das KdoCIR ausgerichtete Öffentlichkeitsarbeit?

26. Wie viele Studienplätze gibt es im Studiengang „Cyber-Sicherheit“ der Universität der Bundeswehr in München, und wie hoch sind die gegenwärtige Auslastung sowie die Abbruchquote innerhalb dieses Studiengangs?

27. Wie viele IT-Angriffe gab es in den letzten fünf Jahren und im Jahr 2018 im Rahmen der Auslandseinsätze auf die Systeme der Bundeswehr (bitte nach Jahren und den einzelnen Auslandseinsätzen der Bundeswehr aufschlüsseln)?

    a) Sofern sich ein Muster erkennen lässt, worauf zielten diese IT-Angriffe im Speziellen ab?

    b) Wie viele dieser Angriffe wurden von Einheiten der Bundeswehr erkannt und abgewehrt?

       Welche Bundesbehörden oder staatlichen Stellen waren in die Abwehr dieser Angriffe in welcher Form involviert?

       Welche Stellen und Behörden anderer Staaten waren in die Abwehr dieser Angriffe in welcher Form involviert?

    c) Welche Schäden wurden verursacht?

28. Im Rahmen welcher Auslandseinsätze der Bundeswehr kamen welche Kräfte des KdoCIR bisher in welcher konkreten Form zum Einsatz?

29. Gab es bis heute – jenseits der Presseberichterstattung über das Eindringen in die internen Netze eines afghanischen Mobilfunkbetreibers im Jahr 2015 (vgl.: www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html) – Aktivitäten der Bundeswehr, im Rahmen derer in fremde oder gegnerische Netze eingegriffen oder gewirkt wurde?

    Wenn ja, welche (bitte konkret aufschlüsseln)?

30. Welche staatlichen und nichtstaatlichen Akteure werden über das Cyber Innovation Hub miteinander vernetzt (bitte aufschlüsseln)?

31. Inwieweit wurden bisher Partnerschaften, gemeinsame Vorhaben, Verträge oder sonstige Kooperationen seitens der Bundeswehr mit welchen Akteuren vereinbart bzw. sind in Zukunft geplant?

32. Was sind die konkreten Ergebnisse der bisherigen Zusammenarbeit mit Start-ups im Rahmen des Cyber Innovation Hub?

    a) Zu welchen konkreten Vereinbarungen ist es bis heute durch dieses Kooperationsinstrument gekommen?

    b) Welche Innovationen haben durch das Cyber Innovation Hub Eingang in das KdoCIR oder andere Organisationsbereiche der Bundeswehr gefunden?

33. Inwiefern hat das Cyber Innovation Hub Projekte durchgeführt, die sich mit sozialen Medien befassen oder diese bedienen?

    Falls ja,

    a) was ist für die Bundeswehr ein Anwendungsfall für die Analyse von sozialen Medien,

    b) wurden Daten deutscher Staatsbürgerinnen und Staatsbürger im Rahmen dieser Projekte verwendet,

    c) wurden diese Projekte ausgeschrieben?

34. Inwiefern bestehen Compliance-Regeln für Beschäftigte des Cyber Innovation Hubs, die etwa den Besitz von Anteilen an Unternehmen betreffen, mit denen das Cyber Innovation Hub Geschäftsbeziehungen unterhält oder aufzubauen plant?

    Unterscheiden sich diese von denen, die im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) oder der BWI GmbH gelten?

    Ist es bisher zu Verstößen gegen diese Regeln gekommen?

35. Wie viele Dienstposten hat das Cyber Innovation Hub, und wie viele dieser Dienstposten sind bereits besetzt?

    a) Wie viele der Dienstposten sind mit einem Absolventen oder einer Absolventin mit universitärem Abschluss in einem MINT-Fach (MINT = Mathematik, Informatik, Naturwissenschaft und Technik) besetzt?

    b) Welches Anforderungsprofil sollen Angestellte des Cyber Innovation Hub erfüllen?

    c) Inwiefern wurden außertarifliche Vereinbarungen für Angestellte des Cyber Innovation Hubs getroffen?

36. In welcher Liegenschaft ist das Cyber Innovation Hub untergebracht, und Kosten in welcher Höhe sind für die Unterbringung des Hubs bisher, und werden voraussichtlich bis zum Ende der Pilotphase anfallen?

37. Wo sieht die Bundesregierung rechtlichen Regelungsbedarf für den Einsatz der Bundeswehr im digitalen Raum, und welche Initiativen sind hierzu ggf. geplant?

38. Erachtet die Bundesregierung die gegenwärtigen parlamentarischen Aufsichts- und Kontrollstrukturen sowie die bisherige Unterrichtungspraxis über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum als ausreichend?

    a) In welchem Gremium bzw. welchem Gremien berichtet die Bundesregierung durch wen dem Parlament vollumfänglich über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr oder durch staatliche Stellen der Bundesebene und ihrer Behörden im digitalen Raum?

b) Wie stellt die Bundesregierung eine umfassende, konsistente und zeitnahe Unterrichtung des Parlaments über das Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum sicher?

c) Hat die Bundesregierung in der Vergangenheit das Parlament vollumfänglich und mit Blick auf alle erfolgten Operationen der Bundeswehr über ein Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum unterrichtet?

Wenn ja, in welchem Gremium hat sie dies getan?

39. Erachtet die Bundesregierung angesichts der zunehmenden Bedeutung des digitalen Raums für militärische Operationen eine Anpassung der rechtlichen Grundlagen für notwendig?

Wenn ja, in welchen konkreten Punkten?

Wenn nein, warum nicht?

40. Definiert die Bundesregierung eine Abgrenzung zwischen defensiven und offensiven Operationen und Fähigkeiten der Bundeswehr?

Wenn ja, entlang welcher Kriterien?

41. Unter welchen konkreten Voraussetzungen erachtet die Bundesregierung den Einsatz von Fähigkeiten zum Eindringen, Wirken oder Angreifen in fremde Netze durch die Bundeswehr im digitalen Raum als möglich und notwendig, und auf welcher rechtlichen Grundlage tut sie das?

42. Wie stellt die Bundesregierung eine Abgrenzung von Innerer und Äußerer Sicherheit im Cyber- und Informationsraum im Rahmen der gesetzlichen Grundlagen sicher?

Welche Einschränkungen ergeben sich hieraus für den Einsatz der Bundeswehr im digitalen Raum?

43. Wie wird die ressortübergreifende Kooperation zur Abwehr von IT-Angriffen durch die Bundesregierung bewertet?

Wo und in welchem Umfang soll diese verbessert werden?

Wann ist mit der Vorlage des im Koalitionsvertrags zwischen CDU, CSU und SPD angekündigten zweiten IT-Sicherheitsgesetzes zu rechnen?

44. Wie weit sind die von der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, am 14. Mai 2018 bei der Bundeswehrtagung angekündigten Pläne zur Schaffung einer Agentur für Disruptive Innovation für Cybersicherheit (ADIC) fortgeschritten, und was sollen die konkreten Aufgaben dieser Agentur sein?

45. Welche Kenntnisse hat die Bundesregierung über Operationen und Fähigkeiten der NATO im digitalen Raum?

46. Wie weit sind nach Kenntnis der Bundesregierung die Planungen für das „Cyber Operations Center“ der NATO inzwischen fortgeschritten?

a) Mit welchen konkreten Zielen und Beiträgen bringt sich die Bundesregierung aktuell und in Zukunft in der weiteren Ausplanung der konkreten Aufgaben des „Cyber Operations Center“ der NATO ein?

b) Durch welche konkreten Maßnahmen hat sich die Bundesregierung bisher innerhalb der NATO dafür eingesetzt, dass Aspekte wie politische Kontrolle und Einhaltung des internationalen Rechts im Ausplanungsprozess beachtet werden?

47. Wie bewertet die Bundesregierung die Gefahr einer fortschreitenden Militarisierung im digitalen Raum, und welche konkreten Maßnahmen hinsichtlich einer Anpassung des Instrumentariums der Rüstungskontrolle an veränderte technologische und sicherheitspolitische Rahmenbedingungen plant sie bis wann zu ergreifen?

48. Welche konkreten Initiativen hat die Bundesregierung bis heute selbst angestoßen oder wesentlich unterstützt, um ein internationales Regelwerk für das Handeln von Streitkräften und Nachrichtendiensten im digitalen Raum auf den Weg zu bringen (bitte einzeln darstellen)?

49. Welche konkreten Vorstellungen hat die Bundesregierung in Anbetracht der technologischen Entwicklung und der Zunahme von Angriffen und militärischen Operationen im digitalen Raum für eine Neu- und Weiterentwicklung von Rüstungskontrollinstrumenten als Teil einer modernen und zukunftsorientierten Sicherheitspolitik?

50. Welches internationale Forum erachtet die Bundesregierung als geeigneten Rahmen, um international breit getragene Verhaltensnormen zu verhandeln?

    Welche Initiativen hat die Bundesregierung an diesen Stellen wann angeschoben?

51. Welche Pläne gibt es seitens der Bundesregierung, sich auf internationaler Ebene für Vereinbarungen zur Sorgfaltsverantwortung für ein friedliches Miteinander im digitalen Raum einzusetzen und, sollte es hier noch keine Pläne geben, warum nicht, und welche alternativen Maßnahmen will man ergreifen?

Berlin, den 6. Juni 2018

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, 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