Deutscher Bundestag **Drucksache 18/11688**

18. Wahlperiode 15.03.2017

Kleine Anfrage

der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, Heike Hänsel, Inge Höger, Andrej Hunko, Dr. Alexander S. Neu, Kathrin Vogler und der Fraktion DIE LINKE.

Strukturen des Organisationsbereichs Cyber- und Informationsraum der Bundeswehr in Nordrhein-Westfalen

Im September 2015 gab die Bundesministerin der Verteidigung, Ursula von der Leyen die Einrichtung eines Aufbaustabes für den Bereich Cyber/IT in der Bundeswehr bekannt. Im entsprechenden Tagesbefehl vom 17. September 2015 heißt es: „Die Bundeswehr hat bereits gute Fähigkeiten im Cyber-Raum und in der Informationstechnologie (IT) – diese sind aber organisatorisch verstreut“. Ziel des Aufbaustabes unter Verantwortung der Staatssekretärin Suder und Leitung des Beauftragten für die Strategische Steuerung Rüstung sei es, einen eigenen, dem Bundesministerium „unmittelbar nachgeordneten“ Organisationsbereich zu schaffen, der diese Fähigkeiten zusammenfasst und bündelt (Bundesverteidigungsministerin Dr. Ursula von der Leyen: Tagesbefehl vom 17. September 2015). Im April legte dieser Aufbaustab seine „Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung“ vor. Darin empfiehlt er „die Einrichtung einer Abteilung Cyber/IT (CIT) im Bundesministerium der Verteidigung (BMVg) zum 1. Oktober 2016 (Grundbefähigung)“ und die „Aufstellung eines militärischen Organisationsbereichs für den Cyber- und Informationsraum mit einer Inspekteurin bzw. einem Inspekteur an der Spitze zum 1. April 2017 (Erstbefähigung)“. Tatsächlich wurde im Oktober 2016 die Ministeriumsabteilung Cyber- und Informationstechnik (CIT) in Berlin in Dienst gestellt und der Leiter des Aufbaustabes, Luftwaffen-Generalmajor Ludwig Leinhos, als zukünftiger Inspekteur des Kommandos Cyber- und Informationsraum (CIRK) bestimmt, das auf der Bonner Hardthöhe stationiert werden soll und mit etwa 230 Dienstposten die Führung von 13 700 Kräften übernehmen soll. Mit eigenem Inspekteur ist dieser Organisationsbereich CIRK den bisherigen Teilstreitkräften nahezu gleichgestellt und hat einen vergleichbaren Umfang wie die Marine.

Der Organisationsbereich CIRK wird sich weitgehend aus bereits bestehenden Einheiten zusammensetzen, von denen viele in Nordrhein-Westfalen stationiert sind. Dazu gehören das ebenfalls auf der Bonner Hardthöhe stationierte Führungsunterstützungskommando (zukünftig Kommando Informationstechnik der Bundeswehr, KdoITBw) sowie die diesem nachgeordneten Einheiten Betriebszentrum IT-System der Bundeswehr (BtrbZ IT-SysBw) in Rheinbach und das Zentrum für Informationstechnik der Bundeswehr in Euskirchen. Das ebenfalls direkt dem Kommando Cyber- und Informationsraum unterstehende Kommando Strategische Aufklärung in Gelsdorf liegt im Landkreis Ahrweiler, Rheinland-

Pfalz, direkt an der Grenze zu Nordrhein-Westfalen. Das ihm unterstehende Zentrum Geoinformationswesen der Bundeswehr (Euskirchen) und das (zukünftige) Zentrum Cyberoperationen (Rheinbach) liegen wiederum in NRW, das Zentrum Operative Kommunikation (Mayen) und die Auswertezentrale Elektronische Kampfführung (Daun) im benachbarten Rheinland-Pfalz (http://cyber-peace.org/2016/04/27/auswertung_aufbaustab_cirk/). Auch mehrere Dienstposten des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr in Koblenz sollen zukünftig dem Kommando Cyber- und Informationsraum unterstellt werden.

Dem Organisationsbereich Cyber- und Informationsraum wird auch die unternehmerische Steuerung der Bundeswehr Informationstechnik GmbH (BWI) als Inhouse-Gesellschaft übertragen. Diese hat ihren Sitz wiederum in Meckenheim, NRW, beschäftigt etwa 2 900 Mitarbeiterinnen und Mitarbeiter und unterhält drei Rechenzentren, 25 Servicecenter, vier User-Help-Desks und drei Betriebskompetenzzentren, viele davon wiederum in NRW. Für die Forschung im Bereich Cyber- und Informationsraum sind die Fraunhofer-Institute für Hochfrequenzphysik und Radartechnik (FHR) sowie für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) auf dem Wachtberg bei Bonn von zentraler Bedeutung für die Bundeswehr. Beide haben in der Vergangenheit umfangreich Grundfinanzierung und Drittmittel aus dem Verteidigungshaushalt erhalten und teilweise in enger Kooperation mit dem Institut für Informatik der Universität Bonn Projekte aus dem Bereich Cyber- und Informationsraum bearbeitet. Zumindest in der Vergangenheit waren die Institute auf dem Wachtberg auch an das Intranet der Bundeswehr angeschlossen (www.wissenschaftsrat.de/download/archiv/7703-07.pdf).

Das Weißbuch des Bundesverteidigungsministeriums von 2016 erklärt im Cyber- und Informationsraum einen Bedarf „defensiver und offensiver Hochwertfähigkeiten, die es kontinuierlich zu beüben und weiterzuentwickeln gilt“ (S. 93). Gleichwohl fehlt es dem Weißbuch an brauchbaren Definitionen, welche Grenzen des Cyber- und Informationsraumes als Aufgabenbereich militärischen Handelns festsetzen. Wörtlich heißt es, „der Cyber- und Informationsraum“ habe sich „zu einem internationalen und strategischen Handlungsraum entwickelt, der so gut wie grenzenlos ist“ (S. 37). „Cybersicherheit und -verteidigung“ seien „eine gesamtstaatliche Aufgabe, die gemeinsam zu bewältigen ist. Dazu gehört auch der gemeinsame Schutz der kritischen Infrastrukturen“ (S.38). Entsprechend werden „Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit“ und „Beiträge zum gesamtstaatlichen Lagebild im Cyber- und Informationsraum“ als „durchgängig wahrzunehmende Aufgaben“ (S. 93) der Bundeswehr definiert, ohne das eine Abgrenzung von zivilen Aspekten der Cybersicherheit erfolgt und eine klare Trennung der Aufgaben zwischen dem Organisationsbereich Cyber- und Informationsraum der Bundeswehr und zivilen Institutionen wie dem – ebenfalls in Bonn ansässigen – Bundesamt für Sicherheit in der Informationstechnik erkennbar wären. Bemerkenswert ist in diesem Zusammenhang, dass das Weißbuch die „Nutzung der digitalen Kommunikation zur Beeinflussung der öffentlichen Meinung – angefangen mit der unerkannten, gezielten Steuerung von Diskussionen in sozialen Netzwerken bis hin zur Manipulation von Informationen auf Nachrichtenportalen“ in unmittelbarem Zusammenhang mit Cyberangriffen nennt und „als Element hybrider Kriegführung“ bezeichnet (S. 37).

Wir fragen die Bundesregierung:

1. Wie viele Dienststellen an welchen Standorten werden zukünftig dem Organisationsbereich Cyber- und Informationsraum zugeordnet und dem Kommando Cyber- und Informationsraum unterstellt (bitte nach Bundesland, Standort und bisheriger Einheit auflisten)?

2. Worin bestehen im Einzelnen die Aufgaben des Zentrums Cyberoperationen der Bundeswehr in Rheinbach, und wie begründet die Bundesregierung deren Eingliederung in den Organisationsbereich Cyber- und Informationsraum?
3. Worin bestehen im Einzelnen die Aufgaben des Zentrums Abbildende Aufklärung in Grafschaft-Gelsdorf, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
4. Worin bestehen im Einzelnen die Aufgaben des Zentrums Operative Kommunikation in Mayen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
5. Worin bestehen im Einzelnen die Aufgaben des Zentrums für Geoinformationswesen in Euskirchen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
6. Worin bestehen im Einzelnen die Aufgaben des Zentrums Cybersicherheit in Euskirchen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
7. Worin bestehen im Einzelnen die Aufgaben des Betriebszentrums IT-Systeme der Bundeswehr in Rheinbach, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
8. Worin bestehen im Einzelnen die Aufgaben der Auswertungszentrale elektronische Kampfführung der Bundeswehr in Daun, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?
9. Welche Einheiten zur elektronischen Kampfführung an welchen Standorten werden zukünftig dem Organisationsbereich Cyber- und Informationsraum zugeordnet und dem Kommando Cyber- und Informationsraum unterstellt, und worin bestehen im Einzelnen ihre Aufgaben?
10. Welche Rolle spielt die Elektronische Kampfführung nach Auffassung der Bundesregierung innerhalb des Cyber- und Informationsraumes, und worin besteht nach ihrer Auffassung der Unterschied zwischen den Aufgaben der Elektronischen Kampfführung und den allgemeinen Aufgaben des Organisationsbereichs Cyber- und Informationsraum?
11. Welche IT-Bataillone der Bundeswehr werden zukünftig an welchen Standorten dem Kommando Cyber- und Informationsraum unterstellt, und worin bestehen im Einzelnen ihre Aufgaben?
12. Welche Beträge erhielten die Fraunhofer-Institute FHR und FKIE (und ihre Vorgängerinstitutionen innerhalb der FGAN) in den vergangenen zehn Jahren seitens der Bundesregierung

    a) als Beitrag zur Grundfinanzierung und

    b) als Drittmittel zur Bearbeitung konkreter Forschungsvorhaben

    (bitte nach Jahr, Institut und Projekt auflisten)?
13. Welche der vom Bundesministerium der Verteidigung (teil-)finanzierten Projekte der Fraunhofer-Institute FHR und FKIE betreffen u. a. die Aktivitäten der Bundeswehr im Cyber- und Informationsraum?
14. An welchen der vom Bundesverteidigungsministerium (teil-)finanzierten Projekte waren Angehörige

    a) der Bundeswehr,

    b) der Universität Bonn,

    c) der BWI GmbH

    beteiligt?

15. Besteht weiterhin eine Anbindung der Fraunhofer-Institute FKIE und/oder FHR an das Intranet der Bundeswehr, und kann die Bundesregierung ausschließen, dass zukünftig kontinuierliche Beiträge zur Sicherheit der IT-Systeme der Bundeswehr von den Fraunhofer-Instituten geleistet werden?
16. Über welche Standorte mit wie vielen Mitarbeiterinnen und Mitarbeiter und welcher technischen Infrastruktur verfügt die BWI GmbH nach Kenntnis der Bundesregierung, und was sind im Einzelnen deren Aufgaben (bitte nach Bundesländern und Standorten auflisten)?
17. Welche dieser Standorte der BWI GmbH umfassen auch militärische Dienststellen (bitte nach Standort, Anzahl der Dienststellen und zugehöriger Einheit auflisten)?
18. Worin besteht die unternehmerische Leitung der BWI GmbH durch das Kommando Cyber- und Informationsraum, und welche Befugnisse haben die militärischen Vorgesetzten gegenüber den zivilen Mitarbeiterinnen und Mitarbeiter?
19. Wie definiert die Bundesregierung hybride Kriegführung und ist die Beteiligung ziviler Angestellter einer in Besitz des Bundes befindlichen GmbH an der Cyberverteidigung aus ihrer Sicht selbst als Tendenz zur Hybridisierung der Verteidigung zu bewerten?
20. Anhand welcher Kriterien werden innerhalb der „gesamtstaatlichen Cybersicherheit“ jene „Verteidigungsaspekte“ identifiziert, deren Bewältigung „durchgängig wahrzunehmende Aufgabe“ der Bundeswehr sind, und wie erfolgt die praktische Aufgabenteilung zwischen der Bundeswehr und zivilen Behörden bei der Gewährleistung von Cybersicherheit?
21. Welche Einheiten und Standorte, die dem Kommando Cyber- und Informationsraum unterstehen, werden in die Erstellung eines gesamtstaatlichen Lagebilds im Cyber- und Informationsraum einbezogen, und welche Stelle ist letztlich für die Erstellung und Übermittlung des militärischen Beitrags hierzu verantwortlich?
22. Welche Einheiten und Standorte, die dem Kommando Cyber- und Informationsraum unterstehen, sind als durchgängig wahrzunehmende Aufgabe an der Gewährleistung gesamtstaatlicher Cybersicherheit beteiligt, und welche Einheiten und Standorte sind allein für den Schutz der Infrastrukturen der Bundeswehr zuständig?
23. Gibt es Einschränkungen für Einheiten und Standorte, die dem Kommando Cyber- und Informationsraum unterstehen, wonach diese nur tätig werden dürfen, sofern ein Angriff durch einen staatlichen Gegner erfolgt und/oder explizit auf Infrastrukturen der Bundeswehr zielt?
24. Zählt es zu den durchgängig wahrzunehmenden Aufgaben von Dienststellen, die dem Kommando Cyber- und Informationsraum unterstehen, die Nutzung der digitalen Kommunikation zur Beeinflussung der öffentlichen Meinung dahingehend zu überwachen, ob es sich hierbei um ein Element hybrider Kriegführung handelt oder handeln könnte?
25. Nach welchen Kriterien wird die Beeinflussung der öffentlichen Meinung als Element hybrider Kriegsführung oder Angriff auf den Cyber- und Informationsraum bewertet, und welche Gegenmaßnahmen sieht das Kommando Cyber- und Informationsraum für diese Fälle vor?

Berlin, den 14. März 2017

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch 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