

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/11688 –**

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

Vorbemerkung der Fragesteller

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).

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)?

Angaben zu Dienststellen und Standorten können der Anlage 1 entnommen werden. Die Dienststellen werden dem Kommando Cyber- und Informationsraum (KdoCIR) zum 1. Juli 2017 truppendienstlich unterstellt.

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?

Die Aufgaben des Zentrums Cyberoperationen (ZCO) umfassen das Aufklären und Wirken im Cyber- und Informationsraum (CIR). ZCO erstellt einen Beitrag zum Cyberlagebild im Rahmen der Warn- und Schutzfunktion der Bundeswehr. Auf dieser Basis werden die Einsätze der Bundeswehr und der Betrieb Inland in der neuen Handlungsdimension CIR unterstützt.

Der CIR als Operationsraum ist eine eigenständige Dimension, vergleichbar den Dimensionen Land, Luft, See und Weltraum. Das ZCO klärt auf und wirkt in der Dimension CIR und ist daher im Organisationsbereich CIR als Dienststelle unterhalb des Kommandos Strategische Aufklärung (KSA) eingegliedert.

3. Worin bestehen im Einzelnen die Aufgaben des Zentrums Abbildende Aufklärung in Grafenschaft-Gelsdorf, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?

Die Zentrale Abbildende Aufklärung (ZAbbAufkl) gewinnt Satellitenbilder aus militärischen Systemen, betreibt dazu das nationale Radarsatellitensystem SAR-Lupe und kooperiert international mit Partnern. Sie wertet Satellitenbilder aus, stellt Produkte für entsprechende Führungsebenen bereit und unterstützt Maßnahmen im Rahmen des Nationalen Risiko- und Krisenmanagements und des Rüstungskontrollvertrags „Offener Himmel“ durch Auswertung von Luft- und Satellitenbildern und Datenaufbereitung.

ZAbbAufkl als Dienststelle des KSA klärt im elektromagnetischen Spektrum als Teil des CIR auf.

4. Worin bestehen im Einzelnen die Aufgaben des Zentrums Operative Kommunikation in Mayen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?

Das Zentrum Operative Kommunikation der Bundeswehr (ZOpKomBw) hat den Auftrag, die Lage im Informationsumfeld mit ihren Möglichkeiten und Risiken auf allen Führungsebenen im Führungsprozess zu analysieren, festzustellen, zu beurteilen und durch zielgerichtete Informationsaktivitäten geplante Wirkungen in diesem Umfeld zu erzielen und diese mit wissenschaftlichen Methoden zu messen.

Mit diesem Aufgabenportfolio zeichnet das ZOpKomBw verantwortlich für den Anteil Informationsumfeld im Rahmen von Einsätzen und nationaler Krisen- und Risikovorsorge. Das Informationsumfeld ist der Anteil des CIR, in dem die Informationen zur Meinungsbildung aufgenommen, verarbeitet und weitergegeben werden. Aus der Verantwortlichkeit des ZOpKomBw für den Anteil Einsätze und Krisen- und Risikovorsorge im Informationsumfeld ergibt sich der Bezug zum Organisationsbereich CIR.

5. Worin bestehen im Einzelnen die Aufgaben des Zentrums für Geoinformationswesen in Euskirchen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?

Das Zentrum für Geoinformationswesen der Bundeswehr (ZGeoBw) ist die zentrale Dienststelle des Geoinformationsdienstes der Bundeswehr (GeoInfoDBw). Von hier aus wird die Arbeit des GeoInfoDBw fachdienstlich gesteuert und alle geowissenschaftlichen Faktoren für die Bundeswehr aus einer Hand bewertet. Der GeoInfoDBw leistet mit seinen Angehörigen und Fähigkeiten die Geoinformations-Unterstützung im gesamten Aufgabenspektrum der Streitkräfte. Diese wird im Regelbetrieb sowie im Einsatz durch den interdisziplinären Ansatz aus 18 verschiedenen Geoinformations-Wissenschaften (Biologie, Ethnologie, Fernerkundung, Geodäsie, Geographie, Geoinformatik, Geologie, Geophysik, Geopolitik, Hydroakustik, Hydrographie, Hydrologie, Kartographie, Klimatologie, Meteorologie, Ökologie, Ozeanographie und Photogrammetrie) gewährleistet. In Zeiten der Digitalisierung nehmen die Bedeutung und die Menge von Geoinformationen stetig zu. Geoinformationen sind Informationen über naturgeografische Gegebenheiten der Erde inklusive ihrer Lufthülle und Gewässer, die mit einem Raumbezug (z. B. Koordinaten in einem geographischen Referenzsystem) versehen sind. Dies sind zum Beispiel die Höhe von Bergen, der Verlauf von Flüssen und Straßen, Windgeschwindigkeit, Lufttemperatur, Seegang und Salzgehalt der Meere. Geoinformationen dienen nicht mehr nur der Herstellung einer traditionellen „Papierkarte“, sondern stellen in Verbindung mit Geoinformationssystemen und deren Analysefähigkeiten sowie im Rahmen der Navigation einen hohen strategischen Wert für die Bundeswehr dar. Für Führungs-, Waffen- und Einsatzsysteme sind zuverlässige, hochaufgelöste und qualitätsgesicherte Geoinformationen eine unverzichtbare Grundlage. Somit ist das ZGeoBw über die Geoinformations-Unterstützung ein Kernelement in der Dimension CIR und stellt unter anderem den Raumbezug als Basis und Brücke zu den Dimensionen Land, Luft und See her.

6. Worin bestehen im Einzelnen die Aufgaben des Zentrums Cybersicherheit in Euskirchen, und worin bestehen die Bezüge zum Organisationsbereich Cyber- und Informationsraum?

Das Zentrum für Cybersicherheit der Bundeswehr (ZCSBw) ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der IT-Services und IT-Systeme der Bundeswehr im CIR unter Umsetzung der Schutzziele der Informationssicherheit als Teil der Cyberverteidigung. Daraus ergibt sich der direkte Bezug zum Organisationsbereich CIR.

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?

Das Betriebszentrum IT-Systeme der Bundeswehr (BITS) ist für die Überwachung und Steuerung des Betriebs des IT-Systems der Bundeswehr, insbesondere für die betrieblichen Aspekte des IT-Servicemanagements verantwortlich. Es ist damit Teil des CIR.

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?

Die Auswertezentrale Elektronische Kampfführung führt und steuert fachlich die Bataillone Elektronische Kampfführung und die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung zur Erfassung, Auswertung und Meldung von Signalen im Elektromagnetischen Spektrum. Die Auswertezentrale Elektronische Kampfführung wertet zudem Erkenntnisse zu militärischen und militärisch-relevanten Kräften und Mitteln aus, teilstreitkräfte- und medienübergreifend, einschließlich der Beurteilung ihrer Leistungsfähigkeit, Einsatztauglichkeit bzw. der Ziele und Absichten ihres Handelns und leitet das daraus resultierende Bedrohungspotenzial ab. Sie leistet damit einen wesentlichen Beitrag zur Warn- und Schutzfunktion der Kräfte im Einsatz.

Die Auswertezentrale Elektronische Kampfführung klärt im elektromagnetischen Spektrum als Teil des CIR auf.

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?

Die Bataillone Elektronische Kampfführung 911, 912, 931 und 932 und die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung werden zukünftig dem Organisationsbereich CIR zugeordnet (Standorte siehe Anlage 1). Sie sind dem KSA unterstellt, welches wiederum direkt dem KdoCIR unterstellt ist. Die Bataillone Elektronische Kampfführung 911 und 931 nehmen Aufgaben in der Fernmelde- und Elektronischen Aufklärung sowie in der Unterstützung von Einsatzverbänden mit Mitteln des Elektronischen Kampfes wahr. Das Bataillon für Elektronische Kampfführung 912 nimmt Aufgaben in der Unterstützung von Einsatzverbänden mit Mitteln des Elektronischen Kampfes sowie Maßnahmen mit seegestützten und luftgestützten Aufklärungsmitteln sowie der Radar- und Richtfunkaufklärung wahr. Das Bataillon für Elektronische Kampfführung 932 nimmt Aufgaben in der Unterstützung von Einsatzverbänden mit Mitteln des Elektronischen Kampfes sowie mobile Funkaufklärung wahr, einschließlich der Unterstützung militärischer Evakuierungsoperationen. Die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung betreibt technisch-wissenschaftliche Analyse und technische Analyse im Rahmen der Technischen Aufklärung der Bundeswehr. Die Zentrale Untersuchungsstelle der Bundeswehr für Technische Aufklärung untersucht, entwickelt, realisiert und stellt Verfahren und prototypische Labormuster auf der Basis wissenschaftlicher Methoden für die Erfassung, technische Analyse, Auswertung und den Elektronischen Kampf für das KSA, die Teilstreitkräfte, das Militärische Nachrichtenwesen und nationale Sicherheitsbehörden mit vergleichbaren Aufgaben bereit.

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?

Die Aufgaben des Organisationsbereiches CIR sind im Informationsumfeld, dem Cyberraum und dem Elektromagnetischen Spektrum verortet, die untereinander Schnittmengen haben. Dabei nutzt die Elektronische Kampfführung das elektro-

magnetische Spektrum, um gegnerische Ausstrahlungen zu erfassen, zu lokalisieren und auszuwerten, sowie durch eigene Störmaßnahmen gegnerischen Kräften die Nutzung des elektromagnetischen Spektrums zu verwehren. Damit stellt die Elektronische Kampfführung eine Teilmenge der Fähigkeiten des Organisationsbereiches Cyber- und Informationsraum in den Domänen Aufklärung und Wirkung dar. Informationen, die mit Mitteln der Elektronischen Kampfführung gewonnen werden, unterstützen die Operationsführung im CIR.

11. Welche IT-Bataillone der Bundeswehr werden zukünftig an welchen Standorten dem Kommando Cyber- und Informationsraum unterstellt, und worin bestehen im Einzelnen ihre Aufgaben?

Angaben zu den Standorten der IT-Bataillone können der Anlage 1 entnommen werden. Auftrag der IT-Bataillone ist die Bereitstellung von IT-Services für die Aufgaben der Bundeswehr.

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?

Die Fragen 12 und 13 werden zusammen beantwortet.

Im Betrachtungszeitraum der vergangenen zehn Jahre, d. h. vom Jahr 2007 bis zum Jahr 2016, ergeben sich folgende Grundfinanzierungszuwendungen des Bundesministeriums der Verteidigung (BMVg) an die FGAN-/Fraunhofer-Institute FHR und FKIE (Betrieb und Invest., alle Angaben in Mio. Euro):

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
FHR	6,9	6,9	9,68	10,07	8,78	9,49	12,05	10,09	10,78	11,08
FKIE	8,95	8,95	9,21	10,34	11,37	11,5	11,01	12,91	11,97	12,66

Im Betrachtungszeitraum der vergangenen zehn Jahre ergeben sich folgende Drittmittel für Auftrags-Forschungs- und Technologie (F&T)-Vorhaben an FHR und FKIE (Studienverträge und Zuwendungen in Mio. Euro):

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
FHR	0,85	1,25	1,72	3,48	4,67	5,76	8,66	6,37	6,79	4,46
FKIE	2,14	2,52	4,15	5,59	7,44	9,44	10,25	11,59	14,39	12,05

In der Frage der eindeutig an FHR und FKIE zugeordneten Projekte wird auf die Anlage 2 verwiesen. Da die dortige Gesamtschau auf zurückliegende Projekte einen weitgehenden Rückschluss auf die Gesamtstrategie der Bundeswehr bei Technologievorhaben erlaubt, ist die Anlage 2 als „VS – Nur für den Dienstgebrauch“ eingestuft.* Die laufenden Nummern 74 und 189 ff. der Anlage 2 weisen

* Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

zudem diejenigen Auftrags-F&T-Vorhaben ((teil-) finanzierte Projekte) bei FGAN/ Fraunhofer FHR und FKIE im Bereich der Informationstechnologien aus, die dem CIR zugeordnet werden können. Die Kenntnisnahme durch Unbefugte könnte für die Interessen der Bundesrepublik Deutschland nachteilig sein.

14. An welchen der vom Bundesverteidigungsministerium (teil-)finanzierten Projekte waren Angehörige
 - a) der Bundeswehr,
 - b) der Universität Bonn,
 - c) der BWI GmbHbeteiligt?

Hinsichtlich der zu den Fragen 12 und 13 ausgewiesenen Auflistung der (teil-) finanzierten Projekte ist wegen des im Wissenschaftsbereich üblichen Selbststeuerungsrechts von Forschungsinstituten keine Aussage über die weitere inhaltliche Mitarbeit in Projekten möglich.

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?

Es bestehen zu den Forschungsinstituten auf dem Wachtberg bei Bonn zwei separate Anbindungen zum Bundeswehr-Netz. Eine aktive Daten-Direkt-Verbindung existiert zwischen Forschungsinstituten auf dem Wachtberg und der Generalmajor Freiherr von Gersdorff Kaserne in Euskirchen. Dabei handelt es sich um eine Anbindung des Fraunhofer-Instituts FKIE an die Simulations- und Testumgebung der Bundeswehr. Bei dieser Anbindung wird das Weitverkehrsnetz der Bundeswehr (WANBw) als Transportnetz genutzt. Eine Anbindung der FKIE an die Teilnehmer oder Dienste des WANBw in der Bundeswehr besteht nicht. Es kann – und soll – nicht ausgeschlossen werden, dass die genannten Institute zukünftig im Rahmen der Grundfinanzierung oder der Beteiligung bei Ausschreibungen Konzepte oder Dokumente für die Bundeswehr erstellen oder Forschungsarbeiten für die Bundeswehr durchführen.

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)?

Zu Standorten und Zahlen der BWI GmbH (BWI Informationstechnik und BWI Systeme) wird auf die Anlage 3 verwiesen. Gegenstand des Unternehmens BWI Informationstechnik GmbH ist laut Gesellschaftsvertrag die technikunterstützte Informationsverarbeitung, die Organisation und der Betrieb von Anlagen und Systemen auf dem Gebiet der IT, die Erbringung von Informations- und Kommunikationsdienstleistungen aller Art und alle damit zusammenhängenden und zweckdienlichen Tätigkeiten. Zu den Aufgaben der BWI Informationstechnik GmbH gehört zunächst die unterbrechungsfreie Fortführung der Leistungen aus dem HERKULES-Vertrag im Rahmen des mit dem BMVg abgeschlossenen Leistungsvertrages „Herkules Folgeprojekt“ (HFP) sowie das Erbringen von Leistungen für andere Bundesressorts im Rahmen der IT-Konsolidierung des Bundes in der Rolle als IT-Systemhaus des Bundes. Hieraus ergeben sich auch die Informationen zur technischen Infrastruktur.

17. Welche dieser Standorte der BWI GmbH umfassen auch militärische Dienststellen (bitte nach Standort, Anzahl der Dienststellen und zugehöriger Einheit auflisten)?

Zu den Standorten wird auf die Anlage 3 verwiesen.

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?

Es besteht keine unternehmerische Leitung der BWI Informationstechnik GmbH durch das Kdo CIR. Die unternehmerische Leitung der BWI Informationstechnik GmbH ist Aufgabe der Geschäftsführung der Gesellschaft. Die unternehmerische Steuerung der BWI Informationstechnik GmbH auf Gesellschafterebene erfolgt über die Abteilung CIT des BMVg.

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?

Die Bundesregierung verwendet den Begriff hybride Kriegführung nicht, sondern nutzt den Begriff hybrider Bedrohung. Bezüglich einer Definition von hybrider Bedrohung verweist auf die Antwort der Bundesregierung zu Frage 1 auf Bundestagsdrucksache 18/8631.

Die zivilen Angestellten der BWI Informationstechnik GmbH sind nicht und werden auch nicht in die Cyber-Verteidigung eingebunden. Gleichwohl leisten Mitarbeiter der BWI IT GmbH im Bereich IT-Sicherheit einen Beitrag zum Schutz der Netze und IT der Bundeswehr. Eine Tendenz zur Hybridisierung der Verteidigung – im Verständnis zivil/militärisch – ist nicht erkennbar.

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?

Unter dem Begriff der Cybersicherheit ist allgemein ein anzustrebender Zustand der IT-Sicherheitslage zu verstehen, bei dem die Risiken, die Deutschland aus dem Cyberraum erwachsen, auf ein tragbares Maß reduziert sind. Als Mittel zur Erreichung von Cybersicherheit gelten z. B. die Ressortaufgaben Cyberabwehr, Cyberverteidigung und Cyberaußenpolitik. Alle Aspekte der gesamtstaatlichen Cybersicherheitsvorsorge sind der Cybersicherheitsstrategie für Deutschland vom November 2016 zu entnehmen.

Für die Cyberverteidigung gilt, dass sie als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr (GG Artikel 87a) ist und den für Einsätze der Bundeswehr geltenden nationalen wie völkerrechtlichen Regelungen unterliegt. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind gemäß Weißbuch 2016 originäre Aufgaben des BMVg und der Bundeswehr. Die Cyberverteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyberraum, die zur Einsatz- und Operationsführung oder zur Abwehr von (militärischen) Cyberangriffen geeignet

und erforderlich sind und damit dem Schutz eigener Informationen, IT sowie jenem Waffen- und Wirksysteme dienen. Dazu gehört auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyberabwehr unter verteidigungsrelevanten Aspekten und Situationen.

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?

Grundsätzlich werden alle dem KdoCIR unterstehenden Einheiten einbezogen. Für die Erstellung und Übermittlung der Lage CIR ist das KdoCIR 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?

Das ZCSBw ist an der Gewährleistung der gesamtstaatlichen Cybersicherheit beteiligt und stellt mit seiner IT-Sicherheitsorganisation den Schutz der Infrastrukturen der Bundeswehr im Sinne der IT-Sicherheit sicher.

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?

Der Einsatz der Bundeswehr im Cyberraum unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Rechtsgrundlage für die Einsätze und Verwendungen der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes (Artikel 87a Absatz 1, 2, 3 und 4; Artikel 24 Absatz 2; Artikel 35 Absatz 2 und 3 GG).

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?

Es existiert keine der Fragestellung entsprechende Aufgabe für den Bereich KdoCIR.

25. Nach welchen Kriterien wird die Beeinflussung der öffentlichen Meinung als Element hybrider Kriegführung oder Angriff auf den Cyber- und Informationsraum bewertet, und welche Gegenmaßnahmen sieht das Kommando Cyber- und Informationsraum für diese Fälle vor?

Es wird auf die Antwort zu Frage 24 verwiesen.

Anlage 1 zu Parl Sts bei der Bundesministerin der Verteidigung Grübel
1880022-V195 vom 5. Mai 2017

Lfd. Nr.	Dienststelle	Bisherige Einheit	Bundesland	Standort
1	Kommando Cyber- und Informationsraum	-/-	Nordrhein-Westfalen	Bonn
2	Kommando Strategische Aufklärung	Kommando Strategische Aufklärung	Rheinland-Pfalz	Grafschaft
3	Zentrum Cyberoperationen	Gruppe Computer Netzwerk Operationen	Nordrhein-Westfalen	Rheinbach
4	Dienstältester Deutscher Offizier / Deutscher Anteil Militärisches Nachrichtenwesen	Dienstältester Deutscher Offizier / Deutscher Anteil Militärisches Nachrichtenwesen	-/-	Huntingdon (USA)
5	Zentrum Operative Kommunikation Bundeswehr	Zentrum Operative Kommunikation Bundeswehr	Rheinland-Pfalz	Mayen
6	Auswertezentrale Elektronische Kampfführung	Auswertezentrale Elektronische Kampfführung	Rheinland-Pfalz	Daun
7	Bataillon Elektronische Kampfführung 911	Elektronischer Kampf Bataillon 911	Schleswig-Holstein	Stadum
8	Bataillon Elektronische Kampfführung 912	Elektronischer Kampf Bataillon 912	Niedersachsen	Nienburg
9	Bataillon Elektronische Kampfführung 931	Elektronischer Kampf Bataillon 931	Rheinland-Pfalz	Daun
10	Bataillon Elektronische Kampfführung 932	Elektronischer Kampf Bataillon 932	Hessen	Frankenberg
11	Zentrale Untersuchungsstelle Bundeswehr Technische Aufklärung	Zentrale Untersuchungsstelle Bundeswehr Technische Aufklärung	Bayern	Hof
12	Zentrum Abbildende Aufklärung	Zentrum Abbildende Aufklärung	Rheinland-Pfalz	Grafschaft
13	Schule Strategische Aufklärung Bundeswehr	Schule Strategische Aufklärung Bundeswehr	Schleswig-Holstein	Flensburg
14	Zentrum für Geoinformationswesen der Bundeswehr	Zentrum für Geoinformationswesen der Bundeswehr	Nordrhein-Westfalen	Euskirchen
15	Kommando Informationstechnik Bundeswehr	Führungsunterstützungskommando Bundeswehr	Nordrhein-Westfalen	Bonn
16	Zentrum für Cybersicherheit der Bundeswehr	Informationstechnikzentrum Bundeswehr	Nordrhein-Westfalen Rheinland-Pfalz	Euskirchen Tle Koblenz
17	Zentrum Softwarekompetenz IT-System der Bw	-/-	Nordrhein-Westfalen u. Sachsen	Euskirchen Tle Dresden
18	Betriebszentrum Informationstechnik-System Bundeswehr	Betriebszentrum Informationstechnik-System Bundeswehr	Nordrhein-Westfalen	Rheinbach
19	Informationstechnikbataillon 281	Führungsunterstützungsbataillon 281	Rheinland-Pfalz	Gerolstein
20	Informationstechnikbataillon 282	Führungsunterstützungsbataillon 282	Rheinland-Pfalz	Kastellaun
21	Informationstechnikbataillon 292	Führungsunterstützungsbataillon 292	Bayern	Dillingen a.d. Donau
22	Informationstechnikbataillon 293	Führungsunterstützungsbataillon 293	Bayern	Murnau a. Staffelsee
23	Informationstechnikbataillon 381	Führungsunterstützungsbataillon 381	Brandenburg	Storkow (Mark)
24	Informationstechnikbataillon 383	Führungsunterstützungsbataillon 383	Thüringen	Erfurt

Lfd. Nr.	Dienststelle	Bisherige Einheit	Bundesland	Standort
25	Dienstältester Deutscher Offizier /Deutscher Anteil 1st NATO Signal Battalion	Dienstältester Deutscher Offizier /Deutscher Anteil 1st NATO Signal Battalion	Nordrhein-Westfalen	Wesel
26	Informationstechnikschule Bundeswehr	Führungsunterstützungsschule Bundeswehr	Bayern	Pöcking
27	Deutscher Anteil Cooperative Cyber Defense Centre of Excellence	Deutscher Anteil Cooperative Cyber Defense Centre of Excellence	-/-	Tallin (Estland)

Anlage 3 zu Parl Sts bei der Bundesministerin der Verteidigung Grübel
1880022-V195 vom 5. Mai 2017

Lfd. Nr.	Standort	Bundesland	Gesamtanzahl Mitarbeiterinnen und Mitarbeiter (Stand: 28.3.2107)	Standort auch militärische Dienststelle?
1	Aachen	Nordrhein-Westfalen	3	Ja
2	Alt Duvenstedt	Schleswig-Holstein	5	Ja
3	Altenstadt	Bayern	2	Ja
4	Amberg	Bayern	1	Ja
5	Augsburg	Bayern	9	Nein
6	Augustdorf	Nordrhein-Westfalen	3	Ja
7	Bad Bergzabern	Rheinland-Pfalz	1	Ja
8	Bad Reichenhall	Bayern	2	Ja
9	Bad Salzungen	Thüringen	1	Ja
10	Berlin	Berlin	143	(Ja) ¹
11	Bonn	Nordrhein-Westfalen	577	(Ja) ¹
12	Bremerhaven	Bremen	5	Ja
13	Bruchsal	Baden-Württemberg	2	Ja
14	Büchel	Rheinland-Pfalz	4	Ja
15	Calw	Baden-Württemberg	1	Ja
16	Cottbus	Brandenburg	4	Ja
17	Delitzsch	Sachsen	1	Ja
18	Donaueschingen	Baden-Württemberg	1	Ja
19	Dresden	Sachsen	4	Ja
20	Eckernförde	Schleswig-Holstein	3	Ja
21	Ehningen	Baden-Württemberg	4	Nein
22	Erding	Bayern	2	Ja
23	Erfurt	Thüringen	22	Ja
24	Erndtebrück	Nordrhein-Westfalen	2	Ja
25	Euskirchen	Nordrhein-Westfalen	2	Ja
26	Feldkirchen	Bayern	2	Ja
27	Frankenberg/SA.	Sachsen	10	Ja
28	Freyung	Bayern	1	Ja
29	Fritzlar	Hessen	15	Ja
30	Fürstenfeldbruck	Bayern	3	Ja
31	Germersheim	Rheinland-Pfalz	12	Ja
32	Gerolstein	Rheinland-Pfalz	2	Ja
33	Glücksburg	Schleswig-Holstein	7	Ja
34	Hamburg	Hamburg	39	Ja
35	Hammelburg	Bayern	3	Ja
36	Hannover	Niedersachsen	75	Ja
37	Hilden	Nordrhein-Westfalen	27	Ja
38	Husum	Schleswig-Holstein	4	Ja
39	Idar Oberstein	Rheinland-Pfalz	16	Ja
40	Ingolstadt	Bayern	19	Ja

Lfd. Nr.	Standort	Bundesland	Gesamtanzahl Mitarbeiterinnen und Mitarbeiter (Stand: 28.3.2107)	Standort auch militärische Dienststelle?
41	Kalkar	Nordrhein-Westfalen	4	Ja
42	Kastellaun	Rheinland-Pfalz	1	Ja
43	Kaufbeuren	Bayern	7	Ja
44	Kiel	Schleswig-Holstein	50	(Ja) ¹
45	Koblenz	Rheinland-Pfalz	67	Ja
46	Köln	Nordrhein-Westfalen	118	Ja
47	Kramerhof	Mecklenburg-Vorpommern	3	Ja
48	Laage	Mecklenburg-Vorpommern	4	Ja
49	Lagerlechfeld/Kleinaitingen	Bayern	3	Ja
50	Landsberg am Lech	Bayern	9	Ja
51	Leipzig	Sachsen	61	(Ja) ¹
52	Lohheide	Niedersachsen	2	Ja
53	Magdeburg	Sachsen-Anhalt	7	(Ja) ¹
54	Mainz	Rheinland-Pfalz	1	Ja
55	Marienberg	Sachsen	1	Ja
56	Märkische Heide	Brandenburg	2	Ja
57	Mechernich	Nordrhein-Westfalen	2	Ja
58	Meckenheim	Nordrhein-Westfalen	505	Ja
59	Meppen	Niedersachsen	3	Ja
60	Müllheim	Nordrhein-Westfalen	2	Ja
61	München	Bayern	593	(Ja) ¹
62	Munster	Niedersachsen	15	Ja
63	Münster Westfalen	Nordrhein-Westfalen	43	Ja
64	Neubrandenburg	Mecklenburg-Vorpommern	17	Ja
65	Neuburg a. d. Donau	Bayern	3	Ja
66	Niederstetten	Baden-Württemberg	2	Ja
67	Nürnberg	Bayern	88	Nein
68	Osterholz-Scharmbeck	Niedersachsen	5	Ja
69	Pfungstadt	Hessen	15	Ja
70	Plön	Schleswig-Holstein	3	Ja
71	Potsdam	Brandenburg	2	Ja
72	Regen	Bayern	2	Ja
73	Regensburg	Bayern	5	Ja
74	Rheinbach	Nordrhein-Westfalen	200	Ja
75	Rheine	Nordrhein-Westfalen	4	Ja
76	Rostock	Mecklenburg-Vorpommern	46	Ja
77	Roth	Bayern	10	Ja
78	Saarlouis	Saarland	2	Ja
79	Schönewalde	Brandenburg	5	Ja

Lfd. Nr.	Standort	Bundesland	Gesamtanzahl Mitarbeiterinnen und Mitarbeiter (Stand: 28.3.2107)	Standort auch militärische Dienststelle?
80	Schortens	Niedersachsen	27	Nein
81	Schwerin	Mecklenburg-Vorpommern	7	Ja
82	Schwielowsee	Brandenburg	40	Ja
83	Seedorf	Niedersachsen	3	Ja
84	Sigmaringen	Baden-Württemberg	26	Ja
85	Sonthofen	Bayern	2	Ja
86	Stadtallendorf	Hessen	5	Ja
87	Strausberg	Brandenburg	153	Ja
88	Stuttgart	Baden-Württemberg	10	Ja
89	Torgelow	Mecklenburg-Vorpommern	4	Ja
90	Trier	Rheinland-Pfalz	1	Ja
91	Ulm	Baden-Württemberg	40	Ja
92	Unna	Nordrhein-Westfalen	5	Ja
93	Veitshöchheim	Bayern	17	Ja
94	Weiden i.d.OPF	Bayern	2	Ja
95	Wesel	Niedersachsen	1	Ja
96	Wildflecken	Bayern	2	Ja
97	Wilhelmshaven	Niedersachsen	89	Ja
98	Wunstorf	Niedersachsen	7	Ja

¹ Gleicher Standort, aber mit z. T. eigener Liegenschaft.

