Deutscher Bundestag **Drucksache 19/23415**

19. Wahlperiode 15.10.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Christian Sauter, Alexander Graf Lambsdorff, Jens Beeck, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/22268 –

Aufstellung der Cyber-Reserve der Deutschen Bundeswehr

Vorbemerkung der Fragesteller

Der Cyber- und Informationsraum (CIR) sowie das dem CIR unterstellte Kommando Cyber- und Informationsraum (KdoCIR) wurden im April 2017 aufgestellt. Dies war notwendig, da trotz der vielen Gelegenheiten, die uns eine vernetzte und digitalisierte Welt im Alltag bietet, zugleich wesentliche Verwundbarkeiten im Cyber- und Informationsraum entstehen. Sowohl staatliche als auch nichtstaatliche Akteure haben die Möglichkeit, IT-Schwachstellen auszunutzen, um an sensible Daten zu kommen.

Auch die Bundeswehr ist als Hochwertziel häufig von dieser Art von Bedrohung betroffen. Allein im Jahr 2017 wurden 2 Millionen Zugriffsversuche an ihren zentralen Internetübergängen erkannt (Bundestagsdrucksache 19/2922). Die Zahlen beweisen nach Ansicht der Fragesteller, dass der Ausbau der Verteidigungsstrategien in diesem Raum für die Sicherheit der Bundesrepublik Deutschland notwendig ist. Aus dieser Anerkennung entstand die Organisationseinheit CIR, die in den letzten drei Jahren stark gewachsen ist. Die Entstehung und Entwicklung der Cyber-Reserve ist dabei eine wesentliche Säule.

Reservisten stellen seit jeher einen entscheidenden Bestandteil der Bundeswehr dar und spielen eine unverzichtbare Rolle in der Sicherheitsvorsorge der Bundesrepublik Deutschland. Durch den regelmäßigen Tausch des zivilen Berufes in eine Tätigkeit innerhalb der Bundeswehr leisten sie einen Beitrag zur Leistungsfähigkeit und zum Leistungsausbau der Bundeswehr. Zur Erweiterung, Verstärkung und bedarfsorientierten Unterstützung des aktiven Cyber-Personals versucht die Bundeswehr daher, eine hochqualifizierte Cyber-Reserve aufzustellen. Das Konzept ist sehr weit gefasst und geht deutlich über eine nur aus „klassischen“ Reservisten bestehende Reserve hinaus. Ziel ist es, den Wissenstransfer zwischen Fachleuten der Bundeswehr und Behörden, der Wirtschaft und der Gesellschaft zu fördern. Deshalb werden nicht nur IT-Experten angefragt, sondern auch Experten und Führungskräfte aus verschiedenen Wirtschaftszweigen sowie ausscheidende Berufs- oder Zeitsoldaten, Seiteneinsteiger und Freiwillige.

Nichtsdestotrotz sind aus Sicht der Fragesteller wesentliche Fragen im Zusammenhang mit der Gewinnung und Einsetzung der Cyber-Reservisten ungeklärt. Der bestehende Mangel an Fach- und Einsatzpersonal, Materialien und der Finanzierung der Bundeswehr sind durchaus öffentlich bekannt. Aufgrund

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 14. Oktober 2020 übermittelt.

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

der steigenden Zahl an IT-Angriffen auf staatliche und zivile Infrastrukturen kann die Bundesregierung nicht ohne wesentliche strukturelle und organisatorische Veränderungen im Aufbau der Cyber-Reserve das neue Jahrzehnt bestreiten. Zum Ausgleich des Personalmangels müssen neue Wege gegangen und verkrustete Strukturen aufgebrochen werden.

1. Welche Bedeutung hat Cyber-Sicherheit und besonders eine funktionierende Cyber-Reserve für die Verteidigungsfähigkeit Deutschlands im Cyber-Raum?

Die Cyber-Sicherheit hat in einer zunehmend durch Digitalisierung geprägten Gesellschaft eine essentielle Bedeutung für die Verteidigungsfähigkeit und gesamtstaatliche Sicherheit Deutschlands im Cyber- und Informationsraum (CIR) . Die Cyber-Reserve ist integraler Bestandteil des Personalumfangs des Organisationsbereichs (OrgBer) CIR und leistet somit einen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge.

2. Seit wann wurde am Konzept einer Cyber-Reserve gearbeitet, welche Meilensteine markieren den Weg der Entwicklung bis zur Aufstellung, und welche sind bis 2030 geplant?

Erste Überlegungen eine Cyber-Reserve zu etablieren wurden in der Cyber-Sicherheitsstrategie für Deutschland 2011 formuliert. Das „Konzept für die personelle Unterstützung der „Cyber-Community“ der Bundeswehr („Cyber-Reserve“)“ wurde darauf aufbauend durch den Generalinspekteur der Bundeswehr am 2. März 2017 gezeichnet.

Die „Strategie der Reserve“, die im Oktober 2019 veröffentlicht wurde, wird gegenwärtig umgesetzt. Ein wesentlicher Baustein der Implementierung ist das Fachkonzept der „Cyber-Reserve zur Personellen Unterstützung des aktiven Cyber-Personals der Bundeswehr“, welches sich derzeit in der finalen Bearbeitung des Bundesministeriums der Verteidigung (BMVg) befindet. Abgeleitet aus diesem Fachkonzept sind weitere Grundlagendokumente zur Implementierung prozessualer und struktureller Verfahren zum Ausbau der Cyber-Reserve in Vorbereitung.

Mit der Aufstellung des Kommando Cyber- und Informationsraum (KdoCIR) und der Unterstellung von bereits existierenden Dienststellen, wie dem Kommando Strategische Aufklärung oder dem Kommando Informationstechnik der Bundeswehr, wurden existente Reservestrukturen für den Bereich Cyber/IT-Dienst in die Cyber-Reserve integriert. Ergänzend wurden durch das gezielte Ansprechen von bislang Ungedienten, die über eine fachliche Expertise im Bereich der Informationstechnologien verfügen, neue Reservistendienst Leistende (RDL) gewonnen.

Mit Blick auf die nächste Dekade steht als weiterer Meilenstein die Etablierung eines flexiblen Kräftedispositivs bei Schadenslagen zur Unterstützung des aktiven Personalkörpers an.

3. Welche in- sowie ausländischen staatlichen und nichtstaatlichen Akteure bedrohen aus Sicht der Bundesregierung die Cyber-Sicherheit der Bundesrepublik Deutschland (bitte detailliert begründen)?

Auf den Verfassungsschutzbericht 2019 und die Polizeiliche Kriminalstatistik der Bundesrepublik Deutschland, Jahrbuch 2019, wird verwiesen.

4. Wie bewertet die Bundesregierung die Äußerungen des Inspekteurs CIR, Generalleutnant Ludwig Leinhos, der sich in einem Interview mit dem rechtlich zulässigen Einsatz der Bundeswehr im Inland und besonders mit der Steigerung der Reaktionsfähigkeit auf Cyber-Angriffe auseinandersetzt (Quellen: https://www.faz.net/aktuell/politik/inland/cyberabwehr-verteidigungsfaelle-bitte-nur-werktags-von-9-bis-17-uhr-16311910.html; https://augengeradeaus.net/2019/06/bundeswehr-plaediert-fuer-digitalen-verteidigungsfall-zur-besseren-cyber-abwehr/)?

   a) Welche Rolle spielt die Cyber-Reserve in diesem Kontext?

Die Fragen 4 und 4a werden gemeinsam beantwortet.

Auf die Antwort zu den Fragen 1 und 2 wird verwiesen.

   b) Ist eine Änderung der rechtlichen Grundlage für den Einsatz der Cyber-Reserve in einem „digitalen Verteidigungsfall“ geplant, um schneller auf Cyber-Angriffe reagieren zu können?

Der Begriff „Digitaler Verteidigungsfall“ wird durch die Bundesregierung nicht verwendet. Er stellt keinen Rechtsbegriff dar, der an rechtliche Voraussetzungen anknüpft oder rechtliche Konsequenzen auslöst. Auf die Antworten der Bundesregierung zu den Fragen 1 und 2 auf Bundestagsdrucksache 19/12235 wird verwiesen, welche eine Befassung mit dem Thema „Digitaler Verteidigungsfall“ beinhaltet.

   c) Warum gibt es, wie von Generalleutnant Ludwig Leinhos angeregt, keine Koordinierungsstelle, die den reibungslosen Übergang von Cyber-Abwehr zu Cyber-Verteidigung sicherstellt?

Eine entsprechende Koordinierung erfolgt derzeit im Rahmen der Zusammenarbeit im Nationalen Cyber-Abwehrzentrum (Cyber-AZ). Dies ist eine Informations- und Koordinierungsplattform, zu deren Kernbehörden derzeit das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), der Militärische Abschirmdienst (MAD), die Bundespolizei (BPOL), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) zählen. Zielsetzung des Cyber-AZ ist der Informationsaustausch zu Cybervorfällen im Rahmen der gesetzlichen Grenzen der teilnehmenden Behörden sowie die Abstimmung von Maßnahmen der Behörden bei Cybervorfällen. Das Cyber-AZ beugt so potentiellen Informationsverlusten bei den Behörden vor und verbessert die Koordination und Abstimmung von Maßnahmen bei Cybervorfällen der teilnehmenden Behörden.

   d) Wie weit ist der Planungsstand des sogenannten Cyberabwehrzentrums Plus“, und wann soll es seine Tätigkeit vollumfänglich aufnehmen?

Beim „Cyberabwehrzentrum Plus“ handelt es sich um einen (Arbeits-)Begriff zur Weiterentwicklung Cyber-AZ, der zuletzt in die Ende 2019 verabschiedete neue Geschäftsordnung des Cyber-AZ mündete. Die dadurch nötigen Anpassungen am Cyber-AZ sind zwischenzeitlich umgesetzt und die vorgesehenen Aufgaben werden wahrgenommen. Die Fortentwicklung des Cyber-AZ bleibt jedoch ein kontinuierlicher Prozess, da sich Technik und Cyber-Gefahren stetig verändern.

e) Anhand welcher Kriterien stellt die Bundesregierung fest, ob ein Cyber-Angriff in die Zuständigkeit der Polizei bzw. der Nachrichtendienste fällt?

Die Zuständigkeit im Cyberbereich bestimmt sich nach denselben Kriterien, die auch außerhalb des Cyberraums gelten. Wie auch in der analogen Welt ist daher für die Frage, welche Behörde im Einzelfall zuständig ist, vor allem entscheidend, ob der betreffende Sachverhalt unter die der jeweiligen Behörde gesetzlich zugewiesenen Aufgaben gefasst werden kann.

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

a) Wie viele Dienstposten sind eingeplant, und wie viele sind derzeit besetzt (bitte jeweils in Dienstgrad und Laufbahn aufschlüsseln)?

Die Fragen 5 und 5a werden zusammen beantwortet.

Reservistinnen und Reservisten leisten Wehrdienst, dabei können sie auch zur temporären Verbesserung der personellen Einsatzbereitschaft der Bundeswehr Aufgaben auf vakanten Dienstposten für Soldatinnen auf Zeit, Soldaten auf Zeit, Berufssoldatinnen oder Berufssoldaten erledigen. Derzeit sind im Organisationsbereich CIR 523 Dienstposten (DP) ausgebracht, die der Cyber-Reserve zuzuordnen sind und die bei Vakanzen mit RDL besetzt werden sollen. Von diesen sind – mit Stand 18. September 2020 – 283 DP mit RDL besetzt. Dies entspricht einer Dienstpostenbesetzung von ca. 54 Prozent.

Im Einzelnen:

- Dienstgradgruppe der Stabsoffiziere

(Major-Oberst)

95 von 158 DP besetzt. Dies entspricht einem Besetzungsgrad von ca. 61 Prozent.

- Dienstgradgruppen der Leutnante und Hauptleute:

113 von 165 DP besetzt. Dies entspricht einem Besetzungsgrad von ca. 68 Prozent.

- Dienstgradgruppe der Feldwebel

(Feldwebel – Oberstabsfeldwebel)

34 von 120 DP besetzt. Dies entspricht einem Besetzungsgrad von ca. 28 Prozent.

- Dienstgradgruppe der Unteroffiziere

(Unteroffizier/Stabsunteroffizier)

11 von 36 DP besetzt. Dies entspricht einem Besetzungsgrad von ca. 31 Prozent.

- Dienstgradgruppe der Mannschaften

(Gefreiter – Oberstabsgefreiter)

30 von 44 DP besetzt. Dies entspricht einem Besetzungsgrad von ca. 68 Prozent.

b) Wie hoch ist der Frauenanteil bei den besetzten Dienstposten, und welchen Prozentsatz hat sich die Bundesregierung als Ziel gesetzt?

Der Frauenanteil über alle Dienstgradgruppen beträgt ca. 8 Prozent. Für den Bereich der „Cyber-Reserve“ besteht derzeit keine von der Zielsetzung des BMVg abweichende Zielsetzung für den Frauenanteil.

c) Welche Maßnahmen ergreift die Bundesregierung zur Personalgewinnung?

Für die Personalgewinnung der Bundeswehr wird mittels eines breiten Medien-Mixes geworben.

Interessentinnen und Interessenten am Arbeitgeber Bundeswehr wenden sich an die Karriereberatung und werden dort umfangreich beraten, betreut und erhalten eine Vielzahl an Informationen zum Berufsbild Soldatin / Soldat, zu Laufbahnen sowie zum Einstellungsverfahren. Auch über Möglichkeiten zum Reservistendienst im Allgemeinen und zur Cyber-Reserve im Besonderen wird an dieser Stelle bei Interesse informiert.

Der Bereich Cyber/IT ist aufgrund seiner besonderen Bedeutung generell ein maßgeblicher Bestandteil der personalwerblichen Kommunikation.

Explizite Werbemaßnahmen für die Cyber-Reserve sind darüber hinaus nicht vorgesehen.

Der jährliche personelle Ergänzungsbedarf im Bereich der Cyber-Reserve wird durch die Personalführung grundsätzlich regelmäßig gedeckt.

d) Wie viele Posten sind derzeit von ungedienten Freiwilligen und Seiteneinsteigern besetzt (bitte jeweils in Dienstgrad und Laufbahn aufschlüsseln)?

Mit Stand vom 18. September 2020, sind insgesamt 19 DP durch gediente Seiteneinsteiger besetzt, die konkret dem Kräftedispositiv Cyber-Reserve zugeordnet sind.

Im Einzelnen:

- Dienstgradgruppe der Stabsoffiziere

(Major-Oberst)

7

- Dienstgradgruppen der Leutnante und Hauptleute

10

- Dienstgradgruppe der Feldwebel

(Feldwebel – Oberstabsfeldwebel)

1

- Dienstgradgruppe der Unteroffiziere

(Unteroffizier/Stabsunteroffizier)

1

e) Wie soll sich voraussichtlich die Anzahl der Dienstposten bis 2025 entwickeln?

Als Folge der in der Strategie der Reserve festgelegten Grundbeorderung aller ausscheidenden Soldatinnen und Soldaten soll der Umfang der DP für die Cyber-Reserve im OrgBer KdoCIR auf 931 anwachsen.

6. Nach welchen Kriterien werden Bewerber der Cyber-Reserve ausgewählt?

a) Welche Voraussetzungen müssen von Cyber-Reservisten bei der Musterung erfüllt werden?

Die Fragen 6 und 6a werden zusammen beantwortet.

Cyber-Reservistinnen und -Reservisten sind Teil der Reserveorganisation der Bundeswehr. Für diese gelten die gleichen gesundheitlichen Anforderungen wie für alle übrigen Reservistinnen und Reservisten. Dabei sind die gesetzlichen und weisungsgemäßen Voraussetzungen hinsichtlich gesundheitlicher und charakterlicher Eignung entsprechend der Personalbedarfsdeckung der Bundeswehr zu erfüllen. Diese orientieren sich bei künftigen Reservistinnen und Reservisten u. a. am bisherigen oder vorherigen Status der Bewerberin oder des Bewerbers (fachliche Eignung festgelegt durch Studium oder Berufsbilder, wehrrechtliche Verfügbarkeit, gesundheitliche Eignung). Ein Erfüllen der gesundheitlichen Voraussetzungen stellt auch im Bereich der Cyber-Reserve sicher, dass eine hinreichende körperliche Belastungsfähigkeit der Soldatinnen und Soldaten für die allgemeinmilitärische, fachliche Ausbildung und anschließende Verwendung auf dem geplanten Dienstposten grundsätzlich sichergestellt ist.

Für Tätigkeiten in der Cyber-Reserve werden keine gesonderten Anforderungen gestellt.

b) Ist eine Absenkung der Voraussetzungen notwendig, um alle Planstellen zu besetzen, und gibt es Überlegungen in diese Richtung?

Eine Absenkung der Voraussetzungen ist aus Sicht des Bundesministeriums der Verteidigung nicht notwendig, da der derzeitige personelle Bedarf unter den aktuellen Voraussetzungen gedeckt werden kann.

c) In welchen Schritten verläuft der Bewerbungsprozess, und wie viele Monate dauert es etwa im Regelfall vom ersten Kontakt seitens des Bewerbers bis zur Ernennung nach erfolgreicher Ausbildung?

Eine allgemeingültige Aussage zur Dauer des Verfahrens ist nicht möglich, da es sich jeweils um eine differenzierte Einzelfallbetrachtung handelt, die sich an der angestrebten Laufbahn wie den individuellen Abholpunkten orientiert.

Grundsätzlich werden die Bewerberinnen und Bewerber nach Information durch die Karriereberatung sowie nach entsprechender Vorauswahl ggf. zu einem Auswahlverfahren eingeladen. Dies führt das hierfür zuständige Karrierecenter durch.

Bei festgestellter Eignung führt das Bundesamt für das Personalmanagement der Bundeswehr eine konkrete Auswahlberatung der Interessenten sowie ggf. die Einplanung in eine entsprechende Laufbahn durch.

Die Dauer dieses Prozesses kann zwischen wenigen Wochen und bis zu einem Jahr liegen. Einfluss darauf haben im Einzelnen u. a. der Zeitpunkt des Bewer-

bungseingangs, die verfügbaren Termine beim Karrierecenter und die zeitliche Verfügbarkeit der Bewerberin/des Bewerbers.

Bis zum erfolgreichen Abschluss der Ausbildung vergehen regelmäßig mehrere Jahre.

7. Was beinhaltet die Ausbildung der Cyber-Reservisten?

   a) Welche Unterschiede sieht die Bundesregierung in der Ausbildung und Tätigkeit der Cyber-Reservisten im Vergleich zu Unternehmen und Hochschulen, die im Bereich Cyber-Sicherheit arbeiten bzw. einschlägige Studiengänge anbieten?

   b) Werden Übungen oder Fortbildungen in Zusammenarbeit mit Unternehmen und Hochschulen aus dem Bereich Cyber-Sicherheit gemacht?

      Falls ja, welche, und was beinhalten sie?

      Falls nein, warum nicht?

   c) Welche Maßnahmen werden ergriffen, um die ständige Weiterbildung der Cyber-Reservisten zu ermöglichen?

Die Fragen 7 bis 7c werden zusammen beantwortet.

Grundsätzlich verfügt das betroffene Personal über eine gleichwertige Ausbildung entsprechend der zivilen Vorgaben in Unternehmen und Hochschulen, die im Bereich Cyber-Sicherheit arbeiten bzw. einschlägige Studiengänge anbieten. Sofern notwendig, erfolgt für Personal in der Cyber-Reserve ohne vorherige militärische Verwendung eine militärfachliche Ausbildung ergänzend und analog zu den aktiven Soldatinnen und Soldaten im Bereich der IT-Experten.

Derzeit werden die konzeptionellen Grundlagen für Verwendungen in der Cyber-Reserve erarbeitet. Erst nach deren Abschluss sind unter Berücksichtigung der entsprechenden Bedarfsträger- und Grundsatzforderungen für Personal der Cyber-Reserve die notwendigen Ausbildungsanteile bzgl. Übungen oder Fortbildungen in Zusammenarbeit mit Unternehmen und Hochschulen aus dem Bereich Cyber-Sicherheit festzulegen.

8. Plant die Bundesregierung das Laufbahnrecht und die Besoldungsordnung für Cyber-Reservisten zu reformieren?

   a) Falls ja, wie, und für welche Zielgruppen?

   b) Falls nein, warum nicht?

Die Fragen 8 bis 8b werden zusammen beantwortet.

Es bestehen derzeit weder Absichten noch Gründe, zukünftig im Bereich der Cyber-Verteidigung eingesetzte Reservistinnen und Reservisten abweichend von den für die übrigen Reservistinnen und Reservisten geltenden Bestimmungen zu behandeln. Dies schließt die nach dem Gesetz über die Leistungen zur Sicherung des Unterhalts von RDL (Unterhaltssicherungsgesetz – USG) zu gewährenden Leistungen mit ein. (RDL fallen nicht in den Anwendungsbereich des Bundesbesoldungsgesetzes.)

Derzeit ist eine Novellierung der Soldatenlaufbahnverordnung geplant, anlässlich derer unter anderem beabsichtigt ist, den Katalog der zivilen Befähigungen für eine Einstellung als Offizierin oder Offizier des militärfachlichen Dienstes um den Strategischen Professional zu ergänzen.

9. Wie viel Geld wird laut der mittelfristigen Finanzplanung bis 2024 jährlich für die Cyber-Reserve zur Verfügung gestellt, und welchen Einfluss hat die Bekämpfung der Auswirkungen der Corona-Pandemie auf die Höhe des Budgets für die Cyber-Reserve?

Die Cyber-Reserve kann – derzeit ohne Einschränkungen – im Rahmen der durch den Haushalt festgelegten zulässigen Höchstzahl an RDL alimentiert werden. Eine gesonderte Bereitstellung von Haushaltsmitteln erfolgt nicht.

10. Wie viele Cyber-Angriffe wurden bereits durch die Cyber-Reserve seit ihrer Gründung erkannt und verhindert bzw. nicht verhindert?

Das Personal der Cyber-Reserve wird in die originären Strukturen der Streitkräfte eingebettet. Eine Zuordnung, welche Schutzmaßnahmen durch Personal der Cyber-Reserve getroffen wurde, erfolgt nicht.

11. Unterstützt die Bundesregierung die Initiative Reservistenarbeitsgemeinschaft Cyber (RAG Cyber) des Verbandes der Reservisten der Deutschen Bundeswehr e. V.?

    a) Falls ja, wie?

    b) Falls nein, warum nicht?

Die Fragen 11 bis 11b werden zusammenbeantwortet.

Das KdoCIR stellt der Reservistenarbeitsgemeinschaft (RAG) Cyber für Zusammenziehungen und Workshops Infrastruktur, wie z. B. Räumlichkeiten, zur Verfügung. Darüber hinaus ist ein inhaltlicher Austausch zu Themen des Cyber-/IT-Bereichs in unterschiedlichen personellen Zusammensetzung in sechs Arbeitskreisen etabliert.

12. In welcher Form bindet die Bundesregierung den Verband der Reservisten der Deutschen Bundeswehr e. V. in die Umsetzung der neuen Strategie der Reserve – Vision 2032+, unter besonderer Bewertung der dort ebenso erwähnten Cyber-Reserve, ein?

Es ist beabsichtigt, nach Fertigstellung des Fachkonzeptes der Cyber-Reserve, die Operationalisierung im Dialog mit den RAG des Verbandes der Reservisten der Deutschen Bundeswehr e. V. (VdRBw) auszugestalten. Zur Umsetzung der Strategie der Reserve finden regelmäßig Gespräche mit dem VdRBw statt.

13. Plant die Bundesregierung, den Vorschlag, einen Teilzeit-Reservedienst anzubieten, um die Attraktivität des Tätigkeitsfeldes zu steigern (siehe: https://www.reservistenverband.de/magazin-die-reserve/joachim-fritz-cyber-reserve/), aufzugreifen, wenn ja, wie, wenn nein, warum nicht?

    a) Wenn ja, wer soll nach Auffassung der Bundesregierung in dieser Zeit die Krankenversicherung zahlen?

    b) Wenn ja, wer soll nach Auffassung der Bundesregierung bei einer Verletzung im Dienst bei einer Teilzeit-Übung zuständig sein?

    c) Steht die Bundesregierung dazu im Austausch mit zivilen Arbeitgebern, und wenn ja, wie bewerten die zivilen Arbeitgeber die Möglichkeit eines Teilzeit-Reservedienstes?

Die Fragen 13 bis 13c werden zusammen beantwortet.

Es besteht die Möglichkeit eines Teilzeit-Reservistendienstes bereits gemäß § 1 Nummer 3 der Soldatinnen- und Soldatenteilzeitbeschäftigungsverordnung in Verbindung mit § 63b des Soldatengesetzes im Rahmen von Wehrdienst zur temporären Verbesserung der personellen Einsatzbereitschaft.

Während der Wehrdienstleistung besteht für RDL in Teilzeit Anspruch auf unentgeltliche truppenärztliche Versorgung.

Aus sozialversicherungsrechtlicher Sicht ist darauf hinzuweisen, dass auch bei einem Reservistendienst in Teilzeit die Ruhensregelung des § 16 Absatz 1 Satz 1 Nummer 2 des Fünften Buches Sozialgesetzbuch – gesetzliche Krankenversicherung – (SGB V) zu beachten ist. Danach ruht der Anspruch auf Leistungen aus der gesetzlichen Krankenversicherung, solange der Versicherte Dienst auf Grund einer gesetzlichen Dienstpflicht oder Dienstleistungen und Übungen nach dem Vierten Abschnitt des Soldatengesetzes leistet. Dies gilt auch bei einem Reservistendienst in Teilzeit für den gesamten Zeitraum der Wehrdienstleistung.

Erleiden RDL in Teilzeit eine gesundheitliche Schädigung im Zusammenhang mit dem Wehrdienst, gelten die Vorschriften über die Beschädigtenversorgung nach dem Soldatenversorgungsgesetz.

Ein Austausch mit der Arbeitgeberseite zu Themen der Reserve findet in diversen Formaten statt. Die Bundeswehr prüft zurzeit, wie dieser Austausch verbessert werden kann. In diese Prüfung können auch erste Erfahrungen mit dem Reservistendienst in Teilzeit einbezogen werden, sofern dieser von RDL geleistet wird, die ansonsten in einem abhängigen Beschäftigungsverhältnis stehen.

14. Orientiert sich die Bundesregierung bei der Aufstellung der Cyber-Reserve an anderen Ländern, und welche Länder sieht die Bundesregierung als Best-Practice-Vorbild?

Seit 2019 besteht eine enge Zusammenarbeit mit der ebenfalls im Aufbau befindlichen Cyber-Reserve der niederländischen Streitkräfte. Ein durch Deutschland geplanter Workshop in diesem Jahr wurde aufgrund der CORONA-Pandemie abgesagt.

Ähnliche konzeptionelle Vorstellungen zu einer Cyber-Reserve existieren in den skandinavischen Ländern sowie Österreich und der Schweiz.

15. In welchem Rahmen tauscht sich die Bundesregierung mit den NATO-Mitgliedstaaten bezüglich der Aufstellung einer Cyber-Reserve aus, und welche Schlüsse zieht sie aus dem bisherigen Austausch?

Die Aufstellung einer Cyber-Reserve der Bundeswehr wird von NATO-Partnern mit Interesse wahrgenommen. Somit erwarten sich Partnerstaaten einen Erkenntnisgewinn durch einen gegenseitigen Austausch im Rahmen bilateraler Gespräche.

Deutschland ist Mitglied im National Reserve Forces Committee (NRFC), dem Forum der NATO, welches sich mit der Internationalen Reservistenarbeit befasst. Im NRFC wurde das Thema „Cyber-Reserve“ Ende 2019 auf Betreiben Deutschlands als Schwerpunkt in die Themenliste aufgenommen. Bisher wurden Grundlagen der jeweiligen Cyber-Reserven ausgetauscht sowie Chancen, Nutzen und Grenzen der Cyber-Reserve diskutiert. Es bestehen erste Ansätze, aus dem „Best Practise“ anderer Nationen zu lernen, jedoch mussten durch die COVID-19 Pandemie alle ab März 2020 geplanten Formate des Forums abgesagt werden. Seit Juni 2020 hat Deutschland den Vorsitz im NRFC über-

nommen. Ein im November als Präsenzveranstaltung geplantes Treffen auf der Ebene Stabsoffizier wurde aufgrund der erneut verschärften COVID-19 Lage abgesagt und wird nun als virtuelle Veranstaltung durchgeführt. Das Thema bleibt weiter Schwerpunkt.

Auf die Antwort zu Frage 14 wird verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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