Deutscher Bundestag **Drucksache 20/5597**

20. Wahlperiode 09.02.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/5070 –

Verteidigung im Cyberraum – EU-Kooperation und aktive Cyberverteidigung

Vorbemerkung der Fragesteller

Um ein hohes Cybersicherheitsniveau in Deutschland zu erreichen, ist laut Cybersicherheitsstrategie des Bundesministeriums des Innern, für Bau und Heimat von 2021 eine „aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik“ notwendig. Aufgrund der grenzübergreifenden Natur des Cyberraums ist der Schutz desselben eine Aufgabe, die nur international, insbesondere gemeinsam in der Europäischen Union, gestemmt werden kann (www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?blob=publicationFile&v=2, S. 7 und S. 119).

Der Cyber- und Informationsraum ist für die Bundeswehr – abgestimmt mit den Verbündeten in der NATO – zu einer neuen Dimension der Verteidigung neben Land, Luft einschließlich Weltraum und See geworden (www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung). Die Bundeswehr ist in dieser Dimension für gegnerische Akteure ein Hochwertziel, dessen Systeme durch das Kommando Cyber- und Informationsraum (KdoCIR) als dafür neu gegründetem militärischen Organisationsbereich daher in vollem Umfang zu schützen sind (www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag).

Andere Staaten bauen ihre offensiven Fähigkeiten im Cyberraum kontinuierlich aus und setzen diese in militärischen Konflikten ein. Russlands Angriffskrieg gegen die Ukraine begann etwa mit einem breiten Cyberangriff auf ein Satellitennetzwerk, sodass Gefechtsstände, aber auch zivile Einrichtungen in der Ukraine nicht mehr mit dem Internet verbunden und damit nur noch eingeschränkt kommunizieren konnten oder gar ihre Funktionsfähigkeit nicht mehr gegeben war (www.stern.de/digital/online/attacken-auf-satelliten--russland-fuehrt-den-krieg-auch-im-all-31853446.html).

Auch Verbündete der Bundesrepublik Deutschland etablieren Strukturen für offensive Operationen im Cyberraum. So wird die United States Army im Jahr 2023 eine Stabsstelle gründen, die explizit dafür vorgesehen ist, die offensiven Kapazitäten im Cyber- und Weltraum zu koordinieren (www.thedefensepost.com/2022/09/01/us-army-offensive-cyber-office/). Dies trage dem Umstand Rechnung, dass die Bedeutung des Cyberraums für die Verteidigungspolitik stetig wachse und die Anforderungen an offensive Cyberoperationen mit ihnen. Frankreich beschreibt in seiner militärischen Cyberdoktrin gar, dass die

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 8. Februar 2023 übermittelt.

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

Fähigkeit, offensive Militäroperationen im Cyberspace durchzuführen, ein Bestandteil sei, um nationale Souveränität zu gewährleisten (http://lignesdedefense.blogs.ouest-france.fr/files/Éléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20offensive%20%20.pdf).

Darüber hinaus haben die Europäische Kommission und der Hohe Vertreter der EU für Außen- und Sicherheitspolitik am 10. November 2022 eine EU-Politik für die Cyberabwehr vorgelegt. Das Dokument verfolgt das Ziel, die Bürgerinnen und Bürger der EU, aber auch die Streitkräfte der Mitgliedstaaten vor Cyberbedrohungen zu schützen. Die Koordinierung und Zusammenarbeit der Mitgliedstaaten im Bereich der Cyberabwehrfähigkeiten soll auf Basis der Vorschläge der Kommission intensiviert werden (https://germany.representation.ec.europa.eu/news/europaische-verteidigung-starken-eu-vorschlage-zur-cyberabwehr-2022-11-10_de).

Die Europäische Kommission fordert die Mitgliedstaaten der EU in ihrem Dokument explizit dazu auf, auch aktive Verteidigungskapazitäten im Cyberraum zu etablieren und die Bereitschaft zu signalisieren, diese auch als Reaktion auf einen Cyberangriff auf einen Mitgliedstaat einzusetzen. Zusätzlich wird zur Entwicklung der Fähigkeiten eine Kofinanzierung über den Europäischen Verteidigungsfonds in Aussicht gestellt www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf, S. 1 und S. 14).

Eine gemeinsame öffentliche Position der aktuellen Bundesregierung zu aktiven Cybermaßnahmen und Cyberinstrumenten ist dagegen nicht bekannt. Gleichzeitig fordert die Bundesregierung jedoch, die Bundeswehr müsse als Akteur im Cyber- und Informationsraum erfolgreich bestehen können – ohne zu sagen, welche Instrumente der Bundeswehr dafür rechtlich und technisch zur Verfügung stehen sollen (www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1, S. 149).

Vor dem Hintergrund der dargestellten Lage ist es für die Fragesteller von Interesse, wie sich die Bundesregierung und die Bundeswehr im Bereich Cyber- und Informationsraum auf die aktuellen Herausforderungen vorbereiten und wie sie zur kürzlich vorgestellten EU-Mitteilung zur Cyberverteidigung vom 10. November 2022 stehen.

Vorbemerkung der Bundesregierung

In den vergangenen Jahren beobachtete die Bundesregierung trotz aller Bemühungen im Bereich der Cybersicherheit eine steigende Zahl erfolgreicher Cyberangriffe (bspw. Ransomware) mit Schäden in Milliardenhöhe. Die Cyberangriffe Russlands im Zusammenhang mit dem völkerrechtswidrigen Angriffskrieg gegen die Ukraine zeigen, dass der Cyberraum gezielt zur Vorbereitung und Begleitung von Konflikten genutzt wird. Hier bleiben die Angriffe und deren Effekte auch nicht auf das Gebiet des unmittelbaren Konfliktes beschränkt.

Deshalb dürften allein präventive Schutzmaßnahmen unzureichend sein, um erfolgreiche Cyberangriffe bzw. deren Schadenswirkung zu verhindern.

Zunehmend bestätigt hat sich auch, dass innere und äußere Sicherheit im Cyberraum nicht mehr trennscharf voneinander abzugrenzen sind. Die Wahrung der Cybersicherheit und die Verteidigung gegen Cyberangriffe sind daher eine gesamtstaatliche Aufgabe, die in enger Zusammenarbeit der zuständigen Stellen zu bewältigen ist.

Bereits in der „Cybersicherheitsstrategie für Deutschland 2016“ wurden die Cyberabwehr (in Federführung des Bundesministeriums des Innern und für Heimat – BMI), die Cyber-Außen/-Sicherheitspolitik (in Federführung des Auswärtiges Amts – AA) sowie die Cyberverteidigung (Bundesministerium der Verteidigung – BMVg) als drei sich ergänzende Mittel zum Erreichen von ge-

samtstaatlicher Cybersicherheit festgehalten. Dieser Grundsatz wurde auch in der „Cybersicherheitsstrategie für Deutschland 2021“ beibehalten.

Cyberabwehr bezieht sich auf die zivile Abwehr aller Formen vorsätzlicher Handlungen, deren Ziel es ist, die Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen mit informationstechnischen Mitteln zu manipulieren, zu beeinflussen oder zu stören und die keinen „bewaffneten Angriff“ im Sinne von Artikel 51 VN-Charta darstellen.

Eine – aktive – Maßnahme der Cyberabwehr, mit dem Ziel, die zum Angriff genutzten informationstechnischen Systeme mit informationstechnischen Mitteln zu manipulieren oder zu stören, bezeichnet die Bundesregierung als „aktive Cyberabwehr“.

Cyberverteidigung umfasst die in der Bundeswehr für die Erfüllung ihres verfassungsgemäßen Auftrages vorhandenen Fähigkeiten. Dies beinhaltet die aktive Verteidigung im Cyberraum durch die Streitkräfte ebenso wie die Schutzmaßnahmen für die im Geschäftsbereich BMVg genutzten Systeme. Die Verteidigungsfähigkeit der Bundeswehr erfordert jedoch auch ein hohes Maß an Resilienz staatlicher Institutionen und Kritischer Infrastrukturen. Cyberabwehrmaßnahmen der Behörden und Schutzmaßnahmen der Betreiber von IT-Systemen sind dabei zentrale Mittel zur Erhöhung der Resilienz.

Von den oben genannten Begriffs- und Zuständigkeitsdefinitionen ist der englische Begriff „Cyber Defense“ abzugrenzen, der auf internationaler Ebene insbesondere in Dokumenten der Vereinten Nationen, der OSZE, der Europäischen Union und der NATO verwendet wird. Dieser Begriff berücksichtigt bspw. nicht die verfassungsrechtlichen Rahmenbedingungen und Zuständigkeiten in Deutschland, so dass eine eindeutige Zuordnung der im englischen und im Deutschen genutzten Begriffe nicht allgemeingültig möglich ist. Der Begriff ist daher im Kontext des Einzelfalls zu deuten, um entscheiden zu können, ob und in welcher Schwerpunktsetzung die Mittel Cyberabwehr und Cyberverteidigung einzusetzen sind.

Die Antworten auf die Fragen folgen der oben aufgezeigten Begriffsdefinition.

Insbesondere Fragen nach Maßnahmen, Perspektiven, Absichten und Fähigkeiten des BMVg und der Bundeswehr wurden hierbei im Sinne des Begriffs Cyberverteidigung beantwortet.

1. Welche Schlussfolgerungen zieht die Bundesregierung aus der Aufforderung der Europäischen Kommission an die Mitgliedstaaten, die Investitionen in Verteidigungskapazitäten im Cyberraum, einschließlich aktiver Cyberverteidigungsfähigkeiten, mit Dringlichkeit und Priorität zu steigern?

Die Gemeinsame Mitteilung der Europäischen Kommission und des Europäischen Auswärtigen Dienstes zu einer „EU Cyber Defence Policy“ wurde am 10. November 2022 veröffentlicht. Diese wird derzeit durch die Bundesregierung detailliert bewertet, um sich mit einer ressortübergreifend abgestimmten deutschen Position in die zuständigen EU-Ratsarbeitsgruppen einzubringen. Schlussfolgerungen des Europäischen Rates werden nicht vor Ende März 2023 erwartet. Danach ist zu entscheiden, welche nationalen Maßnahmen zu treffen sind. Diese sind auch im Zusammenhang mit der Implementierung der Maßnahmen des im März 2022 verabschiedeten „Strategischen Kompass für Sicherheit und Verteidigung“ zu sehen, der ebenso wie die „EU Cyber Defence Policy“ auf die Bereiche der Cyberabwehr, -außenpolitik sowie -verteidigung verweist.

2. Welche Ableitungen trifft die Bundesregierung aus der Aufforderung der Europäischen Kommission an die Mitgliedstaaten, aktive Verteidigungskapazitäten im Cyberraum aufzubauen?

Die Bundesregierung wird den Vorschlag der Europäischen Kommission und des Hohen Vertreters weiterhin sorgfältig prüfen. Ein Ergebnis liegt noch nicht vor.

Im Übrigen wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 sowie auf die Antwort der Bundesregierung auf die Schriftliche Frage 49 des Abgeordneten Henning Rehbaum auf Bundestagsdrucksache 20/4515 verwiesen.

3. Welche aktiven Cyberfähigkeiten benötigt die Bundeswehr nach Ansicht der Bundesregierung in unmittelbarer und mittelbarer Zukunft?

Die Bundesregierung vertritt die Ansicht, dass die Bundeswehr technisch über alle benötigten Fähigkeiten verfügt, die sie zur Wahrnehmung ihrer Aufgaben im Rahmen der Cyberverteidigung benötigt.

Die gemäß konzeptionellem Zielbild vorgegebenen Cyberfähigkeiten sind – zukunftsfähig auf die Erfordernisse der Landes- und Bündnisverteidigung ausgerichtet – im Fähigkeitsprofil der Bundeswehr beschrieben. Dieses wurde zuletzt 2018 im Verteidigungsausschuss vorgestellt.

Auf den Bericht zum Fähigkeitsprofil der Bundeswehr 2018 (Ausschussdrucksache des Verteidigungsausschusses 19(12)190) wird verwiesen. Eine Neufassung befindet sich derzeit im Billigungsprozess.

4. Inwiefern hat die Aufforderung der Europäischen Kommission an die Mitgliedstaaten, aktive Verteidigungskapazitäten im Cyberraum aufzubauen, Auswirkungen auf die Position der Bundesregierung zu aktiven Cyberfähigkeiten im militärischen Bereich?

Auf die Antwort zu Frage 1 wird verwiesen.

5. Was versteht die Bundesregierung unter sogenannten Hackbacks?

Der Koalitionsvertrag führt aus, dass Hackbacks als Mittel der Cyberabwehr abgelehnt werden. Der Begriff Hackback wird von der Bundesregierung jedoch konzeptionell grundsätzlich nicht verwendet.

Gemeinhin werden unter dem Begriff Hackback solche Eingriffe in IT-Infrastrukturen eines (mutmaßlichen) Angreifers verstanden, die keinen definitorischen Beschränkungen unterliegen. So werden von diesem Begriff auch digitale Vergeltungsschläge umfasst. Die gesamte IT-Infrastruktur eines (mutmaßlichen) Angreifers wird als legitimes Ziel eines Hackbacks betrachtet. Hiernach wären bspw. auch Vergeltungsangriffe auf IT-Infrastruktur vorstellbar, die der Versorgung der Bevölkerung des Angreifers dienen (z. B. Energieversorger).

6. Was ist die Position des Bundesministeriums der Verteidigung (BMVg) bezüglich des Einsatzes sogenannter Hackbacks?

Es wird auf die Antwort zu Frage 5 verwiesen.

Aufgrund der dort genannten fehlenden definitorischen Beschränkungen sind Hackbacks kein Mittel militärischer Operationsführung der Bundeswehr.

7. Inwiefern ist die militärische Cyberverteidigung Teil der in Erstellung befindlichen nationalen Sicherheitsstrategie?

Die Erstellung der Nationalen Sicherheitsstrategie ist noch nicht abgeschlossen.

8. Kann ein Angriff im Cyberraum auf ein NATO-Mitglied mit weitreichenden Folgen etwa auf die Energieversorgung o. ä. des Staates aus Sicht der Bundesregierung eine Beistandspflicht gemäß Artikel V des Washingtoner Vertrags begründen?

   a) Wenn ja, würde die Bundesregierung betroffene Verbündete dann mit Mitteln des Kommando Cyber- und Informationsraum (KdoCIR) mit aktiven Cyberabwehrmaßnahmen unterstützen, und wenn ja, mit welchen?

   b) Wenn ja, würde die Bundesregierung auf konkrete Anfrage betroffener Verbündeter mit Mitteln des KdoCIR selbst aktive Cyberabwehrmaßnahmen gegen einen Angreifer durchführen, und wenn ja, welche?

   c) Wenn nein, warum kann dies nicht eine Beistandspflicht gemäß Artikel V des Washingtoner Vertrags begründen?

Die Fragen 8 bis 8c werden zusammen beantwortet.

Ein Angriff im oder durch den Cyberraum auf einen NATO-Mitgliedstaat mit weitreichenden Folgen etwa auf die Energieversorgung kann aus Sicht der Bundesregierung die allgemeine Beistandspflicht aus Artikel 5 des Nordatlantikvertrags auslösen, wenn und soweit der Angriff im oder durch den Cyberraum die Qualität eines bewaffneten Angriffs im Sinne von Artikel 51 der Charta der Vereinten Nation aufweist. Dies wird auch in Absatz 25 des Strategischen Konzepts der NATO von 2022, siehe https://www.nato.int/strategic-concept/, aufgeführt. Die konkret zu ergreifenden Maßnahmen hängen von dem jeweiligen Einzelfall ab. Sie sind nicht auf Mittel des KdoCIR beschränkt. Wenn zur Beendigung des Angriffs erforderlich und angemessen, können die Maßnahmen auch die Anwendung von Waffengewalt umfassen.

Ergänzend wird auf das Positionspapier der Bundesregierung „On the Application of International Law in Cyberspace“ von März 2021 verwiesen (https://www.auswaertiges-amt.de/de/aussenpolitik/themen/internationales-recht/voelkerrecht-aktuelle-dokumente/2221614?openAccordionId=item-2221684-0-panel).

9. Ab welchem Grad der Schwere im Allgemeinen führt ein Angriff im Cyberraum auf ein NATO-Mitglied aus Sicht der Bundesregierung zur Auslösung der Beistandspflicht gemäß Artikel V des Washingtoner Vertrags?

Zur Auslösung der Beistandspflicht wird auf die Antwort zu den Fragen 8 bis 8c verwiesen. Ein Angriff im oder durch den Cyberraum stellt grundsätzlich dann einen bewaffneten Angriff im Sinne von Artikel 51 der Charta der Vereinten Nationen dar, wenn die durch den Angriff hervorgerufenen Effekte nach Umfang und Wirkung (scale and effects) mit einem herkömmlichen kinetischen, bewaffneten Angriff vergleichbar sind. Dazu wird auf das Positionspapier der Bundesregierung „On the Application of International Law in Cyberspace“ von März 2021 verwiesen (https://www.auswaertiges-amt.de/de/aussenpolitik/themen/internationales-recht/voelkerrecht-aktuelle-dokumente/2221614?openAccordionId=item-2221684-0-panel).

Ob ein Angriff im oder durch den Cyberraum die Schwelle zu einem bewaffneten Angriff überschreitet, ist eine Frage des konkreten Einzelfalles.

10. Kann ein Angriff im Cyberraum auf ein EU-Mitglied mit weitreichenden Folgen etwa auf die Energieversorgung o. ä. des Staates aus Sicht der Bundesregierung eine Beistandspflicht gemäß Artikel 42 Absatz 7 des Vertrages über die Europäische Union begründen?

    a) Wenn ja, würde die Bundesregierung betroffene Verbündete dann mit Mitteln des Kommando Cyber- und Informationsraum mit aktiven Cyberabwehrmaßnahmen unterstützen, und wenn ja, mit welchen aktiven Cyberabwehrmaßnahmen?

    b) Wenn ja, würde die Bundesregierung auf konkrete Anfrage betroffener Verbündeter mit Mitteln des KdoCIR selbst einen sogenannten Hackback gegen den Angreifer durchführen, sofern dieser bestimmt wurde?

    c) Wenn nein, wie begründet die Bundesregierung diese Einstellung gegenüber der Bewertung der Europäischen Kommission, dass sich Mitgliedstaaten bei Angriffen im Cyberraum im Sinne der Beistandspflicht gegenseitig unterstützen sollen?

    d) Wenn nein, wie begründet die Bundesregierung diese Einstellung gegenüber der Aufforderung der Europäischen Kommission an die Mitgliedstaaten, aktive Verteidigungskapazitäten im Falle eines Cyberangriffs auf einen Mitgliedstaat koordiniert zum Einsatz zu bringen?

Die Fragen 10 bis 10d werden zusammen beantwortet.

Ein Angriff im oder durch den Cyberraum auf einen EU-Mitgliedstaat mit weitreichenden Folgen etwa auf die Energieversorgung kann aus Sicht der Bundesregierung die allgemeine Beistandspflicht aus Artikel 42 Absatz 7 des Vertrages über die Europäische Union begründen, wenn der Angriff die Qualität eines bewaffneten Angriffs im Sinne von Artikel 51 der Charta der Vereinten Nationen auf das Hoheitsgebiet eines EU-Mitgliedstaates aufweist. Zu dem hierzu erforderlichen Ausmaß des Angriffs und hinsichtlich der zu ergreifenden Unterstützungsmaßnahmen wird auf die Antworten zu den Fragen 8 bis 8c und 9 verwiesen. Zur Begrifflichkeit des Hackbacks wird auf die Antworten zu den Fragen 5 und 6 verwiesen.

11. Sieht die Bundesregierung die Verteidigungsfähigkeit im Cyberraum, wie die Verbündeten in Frankreich, als Bestandteil nationaler Souveränität an?

Die Gewährleistung der inneren und äußeren Sicherheit ist für die Bundesrepublik Deutschland unveräußerlicher Bestandteil nationaler Souveränität. Das betrifft sowohl die Gewährleistung der nationalen Sicherheit im Cyberraum, als auch die Abwehr von inneren und äußeren Gefahren.

Dazu wird auf das Positionspapier der Bundesregierung „On the Application of International Law in Cyberspace“ von März 2021 verwiesen (https://www.auswaertiges-amt.de/de/aussenpolitik/themen/internationales-recht/voelkerrecht-aktuelle-dokumente/2221614?openAccordionId=item-2221684-0-panel).

12. Ist aus Sicht der Bundesregierung bei der Cyberverteidigung von Infrastrukturen die Trennung zwischen zivilen und militärischen Institutionen sowie zwischen zivilem und militärischem Personal weiterhin sinnvoll?

Sowohl für den Schutz ziviler als auch militärischer Infrastrukturen sind grundsätzlich die jeweiligen Betreiber verantwortlich; das gilt auch für Gefahren im Cyberraum.

Der Geschäftsbereich (GB) BMVg wird im konkreten Einzelfall im Rahmen der Cyberverteidigung unterstützend tätig.

Die personelle und organisatorische Verantwortlichkeit ist verfassungsrechtlich konstituiert.

13. Plant die Bundesregierung, Personal der Bundeswehr in Friedenszeiten auch beim Bundesamt für Sicherheit in der Informationstechnik (BSI) einzusetzen, um einen gegenseitigen Austausch zwischen zivilem und militärischem Personal in der Cyberverteidigung zu ermöglichen?

    a) Wenn ja, wo soll das Personal eingesetzt werden?

    b) Wenn ja, zu welchem Zweck soll das Personal eingesetzt werden?

Die Fragen 13 bis 13b werden zusammen beantwortet.

Es wird ein Offizier aus dem Kommando Cyber- und Informationsraum (Kdo-CIR) der Bundeswehr als Fachexperte im Nationalen IT-Lagezentrum des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingesetzt. Diese Besetzung dient dem Zweck, Erkenntnisse zur Cyber-Sicherheitslage und möglicher Bedrohungen zeitnah auszutauschen und mit dem jeweiligen Hintergrundwissen gemeinsam zu bewerten.

14. Plant die Bundesregierung, Personal des BSI im Verteidigungsfall bei der Bundeswehr im Organisationsbereich CIR (Cyber- und Informationsraum) einzusetzen?

    a) Wenn ja, wo soll das Personal eingesetzt werden?

    b) Wenn ja, zu welchem Zweck soll das Personal eingesetzt werden?

Die Fragen 14 bis 14b werden zusammen beantwortet.

Das BSI wird auf Grundlage seiner gesetzlichen Aufgaben und Befugnisse auch für den GB BMVg tätig. Beispielhaft seien hier die §§ 4a, 5a und 8 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) unter Berücksichtigung der jeweiligen Bereichsausnahmen genannt. Eine fallbezogene Amtshilfe des BSI für die Bundeswehr im Verteidigungsfall ist nicht ausgeschlossen und hängt von den Umständen des Einzelfalls ab.

15. Welche Rolle spielt die von der Bundesministerin des Innern und für Heimat, Nancy Faeser, am 12. Juli 2022 vorgelegten Cybersicherheitsagenda für das BMVg?

Das BMVg ist als Träger der Aufgabe Cyberverteidigung integraler Bestandteil gesamtstaatlicher Cybersicherheit. Für viele der Vorhaben der 20. Legislaturperiode im Kontext der Cybersicherheit hat das BMI die Federführung innerhalb der Bundesregierung, unabhängig der Ressorthoheit des BMVg im Bereich Cyberverteidigung.

Die Cybersicherheitsagenda fasst im Sinne dieser Funktion als interne Agenda die aus Sicht BMI wichtigsten Maßnahmen strukturiert zusammen.

Zur Erarbeitung der Inhalte ist eine zeitgerechte Einbindung der von der Durchführung der Maßnahmen betroffenen Ressorts vorgesehen.

Insofern stellt die Cybersicherheitsagenda aus Sicht BMVg die wesentlichen Handlungslinien des BMI transparent dar und ermöglicht so in der inhaltlichen

Ausgestaltung der Vorhaben zielgerichtete Beiträge zur Erhöhung der gesamtstaatlichen Cybersicherheit.

16. Welche Formen der Zusammenarbeit gibt es zwischen der Bundeswehr und den Streitkräften NATO-Verbündeter im Bereich der Verteidigung im Cyberraum?

Im Rahmen der „Operationalisierung der Dimension Cyberspace“ der NATO haben bisher 13 Nationen, darunter Deutschland, ihre Bereitschaft zur Bereitstellung von Effekten im Cyberraum durch Cyberoperationen angezeigt und arbeiten in diesem Rahmen zusammen und führen gemeinsame Übungen durch.

Darüber hinaus wird die Stärkung der Cybersicherheit aller NATO-Nationen durch die Umsetzung des Cyber Defence Pledge erhöht. Dies umfasst zivile sowie militärische Bereiche.

17. Wurde die vom Bundesminister für Digitales und Verkehr, Dr. Volker Wissing, am 10. Mai 2022 angekündigte (www.handelsblatt.com/politik/international/g7-digitalministerkonferenz-westen-sagt-ukraine-unterstuetzung-auch-im-cyberkrieg-gegen-russland-zu/28326012.html) gemeinsame Arbeitsgruppe mit Kanada zur Auswertung von Cyberangriffen durch die Bundesregierung bereits eingerichtet?

18. Wenn ja, wie oft ist die gemeinsame Arbeitsgruppe bereits zusammengekommen?

    a) Wenn nein, wann wird die gemeinsame Arbeitsgruppe eingerichtet?

    b) Inwiefern ist das BMVg in die Gespräche zu dieser Arbeitsgruppe beteiligt?

    c) Inwiefern wird das BMVg in dieser Arbeitsgruppe beteiligt sein?

Die Fragen 17 bis 18c werden zusammen beantwortet.

Auf Basis einer ressortübergreifenden Prüfung wurde die Einrichtung der genannten Arbeitsgruppe verworfen.

Auf die Antwort der Bundesregierung auf die Schriftlichen Frage 187 des Abgeordneten Dr. Reinhard Brandl auf Bundestagsdrucksache 20/4852 wird verwiesen.

19. Welche Formen der Zusammenarbeit gibt es zwischen der Bundeswehr und den Streitkräften EU-Verbündeter im Bereich der Verteidigung im Cyberraum?

Die Zusammenarbeit erfolgt über die durch die European Defense Agency (EDA) bereitgestellten Zusammenarbeitsformate (insbesondere Projekte der Ständigen Strukturierten Zusammenarbeit (PESCO)) im Rahmen der gemeinsamen Teilhabe an EU-Einrichtungen, der Durchführung von EU-Missionen oder -Operationen sowie im Zuge bilateraler Zusammenarbeit in Gesprächsformaten oder Projekten.

Im Rahmen der NATO und den entsprechenden Übungen gibt es eine Zusammenarbeit mit den sieben hier vertretenen Mitgliedstaaten der EU.

20. Welche konkreten Maßnahmen hat das BMVg ergriffen, um die Beschaffungsprozesse im Bereich der IT-Ausstattung zu beschleunigen und zu flexibilisieren, um dem vergleichsweise sehr kurzen Innovationszyklus derselben gerecht zu werden?

Um den Herausforderungen Rechnung tragen zu können, wurde die Digitalisierungsplattform GB BMVg ins Leben gerufen. Diese ist ein Wirkverbund aus Prozessen, Verfahren, Arbeitsweisen und Strukturen im GB BMVg.

Mit einem insbesondere sehr engen Wirkverbund aus Planung und Realisierung wird die Harmonisierung und schnelle Bereitstellung von standardisierten, querschnittlichen und wiederverwendbaren IT-Services konsequent und ganzheitlich umgesetzt. Die zentrale Steuerung durch den Ressort Chief Information Officer (CIO) ermöglicht die zügige und flexible Bedarfsdeckung und beendet ineffizientes Silodenken. Die Digitalisierungsplattform GB BMVg ermöglicht ein Forderungscontrolling von Beginn an. Soweit möglich wird im Bereich der Beschaffung auf handelsübliche IT zurückgegriffen, um lange Beschaffungszeiten durch umfangreiche Entwicklungen zu verhindern.

Um die Verfahren der Planung und Beschaffung von querschnittlichen IT-Services zu optimieren, wurden die so genannten „Clusterprogramme“ eingeführt. Diese bündeln in einem Dokument das strategische Zielbild, den Anteil Mittelfristige Finanzplanung sowie die Bedarfs- und Haushaltsbegründung für alle IT-Services eines Clusters. Sie ersetzen damit drei Dokumente mit ihren organisationsübergreifenden Schnittstellen und stellen die Integration in die Gesamtplanung und Ansteuerung der Bedarfsdeckungsprozesse sicher.

21. Gibt es Pläne vonseiten des BMVg, Neuregelungen der Vergabeverfahren anzustoßen, um IT-Ausstattung zur militärischen Nutzung schneller beschaffen zu können?

Die Möglichkeit zur Beschleunigung von Vergabeverfahren im Oberschwellenbereich für die Beschaffung militärischer Ausrüstung zur unmittelbaren Stärkung der Einsatzfähigkeit der Bundeswehr ist mit dem Inkrafttreten des Gesetzes zur Beschleunigung von Beschaffungsmaßnahmen der Bundeswehr (BwBBG) am 19. Juli 2022 geschaffen worden. Durch die Annahme der Beschlussempfehlung des Wirtschaftsausschusses hat der Bundestag zum Begriff Militärausrüstung (siehe § 104 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen – GWB) klargestellt, dass hiervon sowohl körperliche Sachen im Sinne von § 90 des Bürgerlichen Gesetzbuches (BGB) als auch nichtkörperliche Gegenstände wie etwa Software und Rechte umfasst sind. Der Begriff der Militärausrüstung umfasst damit insbesondere Produkte (Waffen, Munition Kriegsmaterial), die in der Gemeinsamen Militärgüterliste der Europäischen Union aufgelistet sind, ist aber unter der Berücksichtigung der sich weiterentwickelnden Technologie weit auszulegen. Auf Bundestagsdrucksache 20/2644 wird verwiesen.

Insofern besteht mit dem BwBBG die Möglichkeit, IT-Ausstattung unter Einbezug von Software und Rechten zur militärischen Nutzung beschleunigt zu beschaffen, wenn diese Beschaffung der Stärkung der Bündnis- und Verteidigungsfähigkeit entsprechend den strategisch-politischen sowie konzeptionellen Vorgaben dient.

22. Inwiefern plant das BMVg, digitale Souveränität als Vergabekriterium in Vergabeverfahren aufzunehmen?

Unter digitaler Souveränität versteht die Bundesregierung die Fähigkeiten und Möglichkeiten von Staaten oder Staatengemeinschaften, ihre Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können, von der technologischen Souveränität (kritische Komponenten) über Datensouveränität bis hin zur Cybersicherheit und digitalen Infrastrukturen. Digitale Souveränität bedeutet dabei, im Rahmen offener Märkte und des regelbasierten Handels eigene Stärken auszubauen und strategische Schwächen zu reduzieren. Auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/4500 wird verwiesen.

Eine generelle Planung des BMVg, die digitale Souveränität als Vergabekriterium selbst bzw. Kriterien, die die digitale Souveränität fördern, als Kriterien für Vergabeverfahren aufzunehmen, besteht derzeit nicht. Jedes Vergabeverfahren im Bereich Software, Hardware oder IT-Services wird durch die jeweils zuständige Vergabestelle gemäß den jeweiligen Bedarfsanforderungen konzipiert und aufgesetzt. Sofern die in Bezug auf die digitale Souveränität geforderten Ausschreibungskriterien im Einklang mit dem geltenden Vergaberecht stehen, kann der Aspekt der digitalen Souveränität bei der Auswahl des wirtschaftlichsten Angebots (siehe § 127 GWB) berücksichtigt werden.

23. Welche konkreten Maßnahmen ergreift die Bundesregierung, um IT-Ausstattung und Software für die Streitkräfte im Bereich der Cyberverteidigung gemeinsam mit EU-Partnern zu beschaffen?

Der GB BMVg nutzt verschiedene etablierte Formate auf bi- und multinationaler Ebene und Ebene der EU. Dabei spielen insbesondere PESCO und der Europäische Verteidigungsfonds (EVF) als Formate eine wesentliche Rolle, um konkrete Produkte und Bedarfe gemeinsam mit den EU-Mitgliedstaaten zu beschaffen.

Daneben existieren fachspezifische Arbeitsgruppen im Rahmen der EU, v. a. im Rahmen verschiedener Formate der EDA. Hier werden auf fachlicher Ebene Einzelthemen zu aktuellen und zukünftigen Interessenschwerpunkten behandelt. Dabei werden fähigkeitsbezogen gleiche Bedarfe verschiedener Mitgliedstaaten identifiziert, im Vorfeld konkreter Beschaffungsabsichten gemeinsame Lösungsansätze sondiert und gegebenenfalls in den jeweiligen nationalen Beschaffungswegen weiterverfolgt und konkretisiert.

Die konkrete Beschaffung bleibt dabei eine souveräne und einzelfallbezogene Entscheidung, in die Aspekte zu Schlüsseltechnologien, digitaler Souveränität und nationaler Sicherheit mit einfließen.

24. Welche Pläne verfolgt das BMVg, die Anforderungen an IT-Ausstattung und Software für die Streitkräfte im Bereich der Cyberverteidigung mit denjenigen der EU-Partner zu harmonisieren?

Aktive Cyberfähigkeiten werden absehbar aus Gründen des Geheimschutzes auch weiterhin dem nationalen Vorbehalt unterliegen.

Hiervon unbenommen sind die Maßnahmen zur Herstellung der Interoperabilität der Streitkräfte in NATO und EU.

25. An welchen Beschaffungsprojekten im Bereich Cyberverteidigung und Digitalisierung, die vom Europäischen Verteidigungsfonds subventioniert werden, ist die Bundeswehr beteiligt?

Im Rahmen des EVF beteiligt sich der GB BMVg an folgenden Projekten:

- 5G Communication for Peacekeeping and Defence (5G COMPAD),
- EDF-2021-DIGIT-D-MDOC-EDOCC.

Im Rahmen der Ständigen Strukturierten Zusammenarbeit beteiligt sich der GB BMVg an folgenden Projekten:

- Cyber and Information Domain Coordination Centre (CIDCC),
- System for CSDP Missions and Operations,
- European Secure Software Defined Radio,
- GeoMETOC Support Coordination Element.

26. Welche konkreten Maßnahmen gibt es vonseiten des BMVg, die Interoperabilität der Bundeswehr mit den NATO- und EU-Verbündeten im Cyberraum zu verbessern?

Wesentliche Aufgabe des BMVg ist die Landes- und Bündnisverteidigung. Damit ist die Interoperabilität mit den NATO- und EU-Verbündeten von herausragender Bedeutung.

Ein besonderer Fokus liegt dabei auf den Systemen zur Führungsfähigkeit. Hier wird in einem umfassenden Ansatz die Entwicklung von interoperablen Fähigkeiten im NATO-geführten Programm „Federated Mission Networking“ (FMN) vorangetrieben. Die Bundesregierung setzt sich dafür ein, dass sowohl EU-Verbündete als auch die Organisationen der EU an diesem Programm teilhaben können. Mit dem Ziel eines strukturierten Informationsaustausches mit Verbündeten wird in der Entwicklung besonders auch die Cybersicherheit für die militärischen Fähigkeiten im Systemverbund in einer eigenen Arbeitsgruppe berücksichtigt.

27. Welche Maßnahmen unternimmt die Bundesregierung, um im Sinne der Interoperabilität eine harmonisierte Ausbildung in der Cybersicherheit und Cyberverteidigung unter den EU- und NATO-Mitgliedstaaten sicherzustellen?

Das BMVg bietet im Rahmen freier Kapazitäten und unter Berücksichtigung der Informationssicherheit bzw. Sicherheitseinstufungen die Möglichkeit der Teilnahme an Ausbildungen an eigenen Institutionen. Ebenso nutzt das BMVg beispielsweise die Trainingsangebote der NATO Communications and Information Academy, die harmonisierte Ausbildungen für NATO-Mitgliedstaaten und befreundete Staaten anbietet.

Im Rahmen der europäischen Zusammenarbeit werden Kurse des European Security & Defence College genutzt. Hier bringt sich BMVg auch mit eigenen Kursangeboten ein.

Darüber hinaus werden auch bilateral z. B. im Rahmen des (USA-DEU) Cyber Information Technology Engagement Framework gegenseitige Teilnahmen an Ausbildungs- und Übungsmaßnahmen angeboten und wahrgenommen.

28. An welchen militärischen Übungen auf EU-Ebene in Zusammenhang mit der Verteidigung im Cyberraum hat sich die Bundeswehr in den letzten fünf Jahren beteiligt (bitte nach Zeitraum der Übungen, Anzahl teilnehmender Bundeswehrangehöriger und teilnehmenden EU-Mitgliedstaaten aufschlüsseln)?

Die Bundeswehr hat sich in den letzten fünf Jahren an folgenden militärischen Übungen auf EU-Ebene im Zusammenhang mit Verteidigung im Cyberraum beteiligt:

Übung	Zeitraum	Teilnehmer Bundeswehr	Teilnehmende EU-Staaten
MILCERT22	18./19. Januar 2022	8	BEL, BGR, CZE, EST, IRL, GRC, ESP, FRA, HRV, ITA, CYP, LVA, LTU, LUX, HUN, MLT, NLD, AUT, POL, PRT, ROU, SVN, SVK, SWE, FIN
MILCERT21	16. bis 18. Februar 2021	8	BEL, BGR, CZE, EST, IRL, GRC, ESP, FRA, HRV, ITA, CYP, LVA, LTU, LUX, HUN, MLT, NLD, AUT, POL, PRT, ROU, SVN, SVK, SWE, FIN

29. An welchen multinationalen militärischen Übungen in Zusammenhang mit der Verteidigung im Cyberraum hat sich die Bundeswehr in den letzten fünf Jahren beteiligt (bitte nach Zeitraum der Übungen, Anzahl teilnehmender Bundeswehrangehöriger und teilnehmenden Staaten aufschlüsseln)?

Die Bundeswehr hat sich in den letzten fünf Jahren an folgenden multinationalen militärischen Übungen im Zusammenhang mit der Verteidigung im Cyberraum beteiligt:

Übung	Zeitraum	Teilnehmer Bundeswehr	Teilnehmende Staaten
CROSSED SWORDS 2022	5. bis 11.12.2022	1	NATO
CYBER COALITION 2022	28. November bis 22. Dezember 2022	12	NATO, CHE, FIN, IRL, SWE
CYBER PHOENIX 2022	29. August bis 2. September 2022	18	NLD
CRITICAL INFRASTRUCTURE SECURITY SHOWDOWN 2022	18./19. Juli 2022	8	SGP
GRIFFIN SHINING	9. bis 12. Mai 2022	15	NLD
LOCKED SHIELDS 2022	18.bis 22. April 2022	45	NATO, CHE, FIN, IRL, SWE
ARMY CYBER SPARTAN 5	6. bis 10. Dezember 2021	8	GBR
CYBER COALITION 2021	29. November bis 3. Dezember 2021	3	NATO, CHE, FIN, IRL, SWE
GRIFFIN RISING	18. bis 21. Oktober 2021	12	NLD
MULTILATERAL-CYBER – DEFENCE EXERCISE 2021	3. bis 9. Oktober 2021	5	CHE, JOR, AUT, GBR, FRA, NLD, POL, LUX
LOCKED SHIELDS 2020	April 2020	40	NATO, CHE, FIN, IRL, SWE
CYBER COALITION 2019	2. bis 6.12.2019	40	NATO, FIN

Übung	Zeitraum	Teilnehmer Bundeswehr	Teilnehmende Staaten
MULTILATERAL-CYBER – DEFENCE EXERCISE 2019	5. bis 9. August 2019	5	AUT, ISR
LOCKED SHIELDS 2019	April 2019	35	NATO, CHE, FIN, IRL, SWE

30. Gibt es ein gemeinsames Lagebild des militärischen Cyberraums auf EU-Ebene?

    a) Wenn ja, bei welcher EU-Institution ist dieses angesiedelt?

    b) Wenn ja, wer trägt vonseiten der Bundeswehr zu diesem gemeinsamen Lagebild bei?

    c) Wenn nein, gibt es Pläne, ein solches gemeinsames Lagebild zu etablieren?

Die Fragen 30 bis 30c werden zusammen beantwortet.

Nach Kenntnis der Bundesregierung gibt es derzeit kein gemeinsames Lagebild des militärischen Cyberraums auf EU-Ebene. Ergänzend wird auf die Gemeinsame Mitteilung des Hohen Vertreters über die EU-Politik zur Cyberabwehr vom 10. November 2022 (https://www.eeas.europa.eu/eeas/joint-communication-european-parliament-and-council-eu-policy-cyber-defence_en) verwiesen, in welcher unter anderem explizit die Absicht zur Stärkung der eigenen Fähigkeiten für ein „gemeinsames Lagebild des Cyber- und Informationsraumes auf EU-Ebene“ erwähnt wird. Dieses solle auf dem PESCO-Projekt CIDCC aufbauen. Deutschland hat dieses PESCO-Projekt bereits im Jahr 2019 vor dem Hintergrund vorgeschlagen, dass die vorhandenen Fähigkeiten auf EU-Ebene nicht mehr zeitgemäß sind. Dieser Auffassung haben sich die EU-Mitgliedstaaten unter anderem durch die Annahme des „EU Concept on Cyber Defence for EU-led military Operations and Missions“ [02.05.2022] zwischenzeitlich angenähert. In dem PESCO-Projekt CIDCC beabsichtigt Deutschland als Projektkoordinator zusammen mit den Projektnationen Frankreich, Ungarn und den Niederlanden sowie weiteren aktiven Beobachternationen, eine solche Fähigkeit initial aufzubauen, zu erproben und im Einverständnis aller EU-Mitgliedstaaten bis 2026 in die EU-Strukturen überführt zu haben. Der deutsche Beitrag wird hierbei maßgeblich aus dem Organisationsbereich CIR bereitgestellt.

31. Wer ist nach Kenntnis der Bundesregierung für die Verteidigung gegen Cyberangriffe auf Institutionen der EU zuständig?

Grundsätzlich obliegt der Schutz vor Gefahren im Cyberraum (bspw. Festlegung der eigenen Cybersicherheitsanforderungen, Umsetzung der eigenen Sicherheitsmaßnahmen) der jeweiligen Institution. Das IT-Notfallteam für EU-Institutionen und die Agentur der Europäischen Union für Cybersicherheit sind die wesentlichen Stellen zur Unterstützung dieser Institutionen im Bereich der Cybersicherheit.

Darüber hinaus können EU-Institutionen durch die Sicherheitsorgane des jeweiligen Gastlandes unterstützt werden. Dies umfasst auch Maßnahmen der Cyberabwehr und Cyberverteidigung. Ergänzend wird auf den Sonderbericht des Europäischen Rechnungshofs aus dem Jahr 2022 verwiesen (https://op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/de/).

32. Welche Form der Kooperation gibt es zwischen den „military Computer Emergency Response Teams“ der EU-Mitgliedstaaten?

Über die EDA haben die EU-Nationen das Format „Project Team Cyber Defence“ etabliert, in welchem sich Vertreter militärischer Computer Emergency Response Teams (CERT) oder vergleichbarer Einrichtungen der EU-Nationen zu wechselnden Themen austauschen und gemeinsame Übungen und Veranstaltungen (insbesondere im Zuge der regelmäßigen EU MilCERT Interoperability Conference) organisieren.

Durch die kürzliche Einrichtung des EDA-Projektes „Military Cyber Emergency Response Team operational Network“ (MICNET), initiiert durch EU-Nationen des besagten „Project Team Cyber Defence“, soll diese Zusammenarbeit weiter gestärkt und gemeinsame Standards sowie Hilfsmittel entwickelt werden. Deutschland hat als eine von 18 EU-Nationen am 15. November 2022 die Projektvereinbarung gezeichnet. Die Umsetzung wird im Laufe des Jahres 2023 beginnen.

Darüber hinaus unterhält das deutsche military CERT, als Teil der nationalen und internationalen CERT-Community, mittelbare und unmittelbare, regelmäßige und situationsbezogene Arbeitskontakte zu anderen (nicht nur militärischen) CERT.

33. Wieso beteiligt sich die Bundesregierung nicht am Projekt „Cyber Rapid Response Teams and Mutual Assistance in Cyber Security“ der Ständigen Strukturierten Zusammenarbeit?

Im Rahmen einer Kosten-/Nutzen-Abwägung und unter Berücksichtigung der verfügbaren Ressourcen wurde seitens BMVg einer Teilhabe am EDA-Projekt MICNET der Vorzug gegeben. Auf die Antwort zu Frage 32 wird verwiesen.

34. Gibt es Pläne vonseiten der Bundesregierung, deutsche Unternehmen aus den Branchen Cybersicherheit und Cyberverteidigung konkret zu unterstützen, um das Know-how dieser zukunftsweisenden Technologien in Deutschland zu erhalten?

Die Investitionsprüfung nach dem Außenwirtschaftsgesetz und der Außenwirtschaftsverordnung trägt zur Verhinderung des Abflusses sensibler Technologien oder kritischen Know-hows ins Ausland bei. Zudem werden innovative Unternehmen bei der Entwicklung und Erprobung neuer, softwaregesteuerter Netztechnologien gezielt gefördert, um bei den zukünftigen Kommunikationstechnologien 5G und perspektivisch 6G in der Weltspitze als Technologieanbieter eine führende Rolle einnehmen und die digitale Souveränität stärken zu können (vgl. Ergebnis des Koalitionsausschusses vom 3. Juni 2020 – „Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken“, Nr. 45).

Darüber hinaus erfolgt eine Förderung auf Grundlage des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“. Gefördert werden Verbundprojekte, an denen zahlreiche deutsche Unternehmen aus der Cybersicherheitsbranche beteiligt sind, um Know-how aufzubauen und Grundlagen für Technologien, Produktinnovationen und neue Geschäftsmodelle zu schaffen.

Forschungs- und Bedarfsdeckungsaktivitäten des Bundesministeriums der Verteidigung und seines Geschäftsbereiches erfolgen bedarfsbezogen mit Blick auf das Fähigkeitsprofil der Bundeswehr. Technologiebezogene Einzelmaßnahmen in diesem Zusammenhang können dabei eine wirtschaftsfördernde Wirkung in den entsprechenden Technologiebereichen zur Folge haben. Eine darüber hi-

nausgehende Wirtschaftsförderung bzw. Unterstützung von Unternehmen der Branchen Cybersicherheit und Cyberverteidigung ohne unmittelbaren Nutzen für Projekte der Bundeswehr ist damit jedoch nicht verbunden.

Zum Erhalt und zur Festigung der digitalen Souveränität werden deutsche Firmen aus den Branchen Cybersicherheit und Cyberverteidigung durch die Vertretungen bei NATO und EU dabei unterstützt, sich mit ihrem Produktportfolio bei der Mitgestaltung internationaler IT-Systeme einzubringen.

35. Welche Maßnahmen unternimmt die Bundesregierung, um deutsche und europäische Start-ups in den Branchen Cybersicherheit und Cyberverteidigung zu unterstützen, um die Innovationskraft in diesem Bereich zu erhalten?

Das BMVg hat 2017 den Cyber Innovation Hub der Bundeswehr (CIHBw) ins Leben gerufen. Diese Innovationseinheit soll durch gezielte Marktbeobachtung und Identifikation von Innovationen und Technologietrends im Bereich Cyber/IT neue Ideen und existierende Lösungen erkennen, validieren und gegebenenfalls weiterentwickeln lassen, um diese der Bundeswehr zur Einführung vorzuschlagen. Darüber hinaus fungiert der CIHBw für Start-up-Unternehmen und andere innovative Marktteilnehmer als Schnittstelle und „Marktplatz“ zur Bundeswehr. Dementsprechend findet der CIHBw auch in der von der Bundesregierung 2022 beschlossenen Start-up-Strategie Erwähnung.

Prägendes Merkmal für den CIHBw ist es, nach dem Vorbild vergleichbarer Einheiten in der Wirtschaft und anderer Streitkräfte, einen angemessenen Freiraum mit Handlungsmöglichkeiten für Innovationsvorhaben der Bundeswehr zu etablieren. Dabei arbeitet der CIHBw eng mit Start-ups zusammen und wendet agile Arbeitsmethoden an. Seit seiner Gründung hat der CIHBw mehr als 150 Innovationsvorhaben auch in Zusammenarbeit mit Start-ups angestoßen und trägt so dazu bei, die Innovationskraft im Bereich Cyber/IT zu erhalten, weiter auszubauen und damit mittelbar auch Start-ups zu unterstützen.

Zusätzlich wurde in Kooperation zwischen dem BMVg und dem BMI die Agentur für Innovation in der Cybersicherheit GmbH („Cyberagentur“) gegründet. Die Cyberagentur richtet sich bei ihren Beauftragungen grundsätzlich auch an Start-ups. Ausschreibungen werden in Anlehnung an § 97 Absatz 4 GWB Start-up-freundlich gestaltet. Insbesondere die Aufteilung in Teil- und/oder Fachlose soll Start-ups zur Mitwirkung an Cyberagentur-Projekten ermutigen. Mit dem Nationalen Koordinierungszentrum für Cybersicherheit (NKCS) unterstützen das Bundesministerium für Wirtschaft und Klimaschutz (BMWK), BMI, Bundesministertium für Bildung und Forschung (BMBF) und BMVg insbesondere innovative Start-ups in den Feldern Cybersicherheit und Cyberverteidigung und stärken so die deutsche Sicherheitswirtschaft. Wegen dieser Start-up-Orientierung ist das NKCS auch eine Maßnahme der Start-up-Strategie der Bundesregierung zur Stärkung des Start-up-Ökosystems. Auch werden innovative Start-ups im Bereich Cybersicherheit mit der Initiative „StartUpSecure“ durch das BMBF gefördert.

36. Bewertet die Bundesregierung eine eigenständige deutsche und europäische Cybersicherheits- und Cyberverteidigungsbranche als notwendig, um die Landes- und Bündnisverteidigung auch im Cyberraum sicherzustellen?

Auf die Antworten zu den Fragen 11, 34 und 35 wird verwiesen. Die Notwendigkeit einer eigenständigen deutschen und europäischen Cybersicherheits- und Cyberverteidigungsbranche ergibt sich bereits aus dem Anspruch, bei den zu-

künftigen Kommunikationstechnologien 5G und perspektivisch 6G als Technologieanbieter eine weltweit führende Rolle einzunehmen und damit die digitale Souveränität Deutschlands und Europas zu stärken (vgl. Ergebnis des Koalitionsausschusses vom 3. Juni 2020 - „Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken“, Nr. 45). Darüber hinaus ergibt sich die Notwendigkeit auch aus dem Bedarf einer gesicherten Verfügbarkeit (vgl. Einschränkungen der weltweiten Lieferketten als Folge der Corona-Pandemie).

37. Plant die Bundesregierung, Teile der Branchen Cybersicherheit und Cyberverteidigung als Schlüsseltechnologien zu definieren?

Auf der Grundlage des Strategiepapiers der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie wurden bereits einige Aspekte der Cybersicherheit und Cyberverteidigung als Schlüsseltechnologie definiert. Hierzu gehören neben den sicherheitsrelevanten IT- und Kommunikationstechnologien unter anderem auch die Kryptographie und Kryptotechnologie.

38. Wie hoch beziffert die Bundesregierung die Fördermittel, die sie für Forschungs- und Entwicklungskapazitäten für Innovationen in der Dual-Use-Technologie in den kommenden fünf Jahren aufbringt (bitte nach Jahren aufschlüsseln)?

Die Wehrtechnische Forschung und Technologie (F&T) orientiert sich ausschließlich am Bedarf der Bundeswehr. Es wird keine gezielte Förderung von Dual-Use-Technologien durchgeführt. Die Wehrtechnische F&T greift lediglich im Rahmen von Dual-Use zivile Technologien auf und adaptiert diese für den Bedarf der Bundeswehr.

39. Welche Maßnahmen ergreift die Bundesregierung, um die parlamentarische Kontrolle über den Einsatz von Cyberfähigkeiten der Bundeswehr zu gewährleisten, wie sie es in ihrem Koalitionsvertrag (S. 149) fordert?

Im Koalitionsvertrag (S. 149) haben sich die Regierungsparteien dazu bekannt, dass die parlamentarische Kontrolle über den Einsatz von Cyberfähigkeiten der Bundeswehr gewährleistet sein muss.

Die Bundeswehr unterliegt einer umfassenden, verfassungsrechtlich vorgegebenen parlamentarischen Kontrolle. Dies betrifft die militärischen Fähigkeiten in der Dimension Cyber- und Informationsraum in gleicher Weise wie die anderen militärischen Fähigkeiten der Bundeswehr. Somit unterliegen die Cyberfähigkeiten der Bundeswehr derselben parlamentarischen Kontrolle wie andere militärische Fähigkeiten. Auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/10336 wird verwiesen.

Die parlamentarische Kontrolle erfolgt dabei maßgeblich durch den Verteidigungsausschuss des Deutschen Bundestages, der grundsätzlich jederzeit und auf parlamentarische Initiative sämtliche Vorgänge des Verteidigungswesens untersuchen und sich gemäß Artikel 45a Absatz 2 des Grundgesetzes (GG) zudem jederzeit als Untersuchungsausschuss einsetzen kann. Neben der Kontrolle durch Festlegung der zahlenmäßigen Stärke und der Grundzüge der Organisation der Streitkräfte gemäß Artikel 87a Absatz 1 Satz 2 GG sowie durch den verfassungsrechtlichen Parlamentsvorbehalt für den Einsatz bewaffneter Streitkräfte, der sich auch auf Cyberfähigkeiten erstreckt, ergibt sich eine weitere verfassungsrechtlich garantierte Kontrollmöglichkeit des Parlaments aus dem allgemeinen Frage- und Informationsrecht des Deutschen Bundestages. Bei der

parlamentarischen Kontrolle über die Streitkräfte und somit auch über Cyberfähigkeiten wird der Deutsche Bundestag gemäß Artikel 45b Satz 1 GG durch die Wehrbeauftragte des Deutschen Bundestages unterstützt.

Darüber hinaus erstellt das BMVg seit 2018 jährlich den „Sachstandsbericht Cyber- und Informationsraum“.

40. Wie plant die Bundesregierung, der zunehmend unklarer werdenden Grenze zwischen militärischer und ziviler Dimension im Cyberspace Rechnung zu tragen, um kritische Infrastruktur im Cyberraum zu schützen?

In Bezug auf die Verantwortlichkeiten zum Schutz von Infrastrukturen wird auf die Antwort zu Frage 12 verwiesen. Wie in der Cybersicherheitsstrategie für Deutschland 2021 ausgeführt, zielt die Bundesregierung daher auf eine enge Zusammenarbeit und Informationsaustausch zwischen Wirtschaft und den zuständigen staatlichen Stellen ab.

In Bezug auf die staatlichen Zuständigkeiten wird auf die Vorbemerkung der Bundesregierung verwiesen.

41. Gibt es konkrete Pläne einer Zusammenarbeit zwischen der Bundeswehr und Trägern ziviler kritischer Infrastruktur, etwa im Sinne eines Know-how-Transfers?

Wie andere staatliche Institutionen auch, ist die Bundeswehr Nutzer ziviler kritischer Dienstleistungen wie bspw. der Stromversorgung. In diesem Sinne arbeitet die Bundeswehr als Kunde bereits jetzt mit zahlreichen Trägern ziviler kritischer Infrastruktur zusammen.

42. Gibt es vor dem Hintergrund, dass Streitkräfte auf zivile kritische Infrastruktur im Sinne der Mobilität, Kommunikation und Energieversorgung angewiesen sind, Pläne für einen militärischen Schutz ziviler kritischer Infrastruktur im Cyberraum?

In Bezug auf die Zuständigkeiten wird auf die Antwort zu Frage 12 verwiesen.

Diese Zuständigkeiten führen aus Sicht der Bundesregierung zu einem ausreichend hohen Schutzniveau.

43. Wird die Bundeswehr aufgrund ihrer Fähigkeiten künftig auch für den Schutz von Telekommunikationskabeln am Meeresgrund zuständig sein oder hier eine unterstützende Funktion wahrnehmen?

Der Schutz der Telekommunikationsinfrastruktur obliegt den Betreibern. Diese müssen angemessene technische und organisatorische Maßnahmen zum Schutz gegen Störungen und zur Beherrschung von Sicherheitsrisiken ergreifen.

Diese Vorgaben erstrecken sich auch auf Unterseekabel, soweit diese dem nationalen Recht unterliegen.

44. Welche Rolle schreibt die Bundesregierung zivilen Akteuren in der Verteidigung Deutschlands im Cyberraum zu?

Die in der Antwort zu Frage 12 dargestellten Verantwortlichkeiten zum Schutz von Infrastrukturen gegen Gefahren im Cyberraum bleibt auch im Rahmen der Verteidigung grundsätzlich erhalten.

45. Wie ist der Sachstand der Entwicklung und des Aufbaus sicherer Quantenkommunikationsnetze der Bundeswehr?

Die Bundeswehr betrachtet das Thema Quantenkommunikation bisher ausschließlich im Rahmen der universitären Forschung (Universität der Bundeswehr München (UniBw M)) und im Rahmen von F&T zur Analyse der militärischen Relevanz dieser Technologie.

46. Wie viele Dienstposten für IT-Fachkräfte im Bereich Cyber- und Informationsraum der Bundeswehr sind in den Jahren 2021, 2022 und 2023 vorgesehen, und wie viele davon werden voraussichtlich unbesetzt bleiben?

Im Jahr 2021 (Stichtag: 31. Dezember 2021) waren von insgesamt 5 395 Dienstposten (DP) für IT-Fachkräfte im Organisationsbereich Cyber- und Informationsraum 4 107 besetzt (unbesetzt: 1 288). Für das Jahr 2022 (Stichtag: 31. Dezember 2022) waren von 5 962 DP 4 477 besetzt (unbesetzt: 1 485). Der Organisationsbereich Cyber- und Informationsraum befindet sich weiter in der Umstrukturierung, so dass auch im Jahr 2023 leichte Veränderungen in den DP-Umfängen zu erwarten sind. Für 2023 ist davon auszugehen, dass sich der DP-Besetzungsgrad, insbesondere durch Zuversetzung von derzeit noch in Ausbildung gebundenem Personal, verbessern wird.

47. Was ist der Personalansatz im Computer Emergency Response Team der Bundeswehr (CERTBw)?

Die Bundeswehr hat für drei Incident Response Teams insgesamt zwölf DP im Zentrum für Cybersicherheit der Bundeswehr ausgeplant. Hinzugezogen wird im Bedarfsfall noch aktives Personal, welches originär andere Aufgaben versieht. Zusätzlich baut die Bundeswehr derzeit eine schnell einsetzbare Reserve für Incident Response auf.

48. Was ist der Personalansatz im Computer Emergency Response Team Bund?

Beim Computer Emergency Response Team Bund im Fachbereich OC 2 des Bundesamtes für Sicherheit in der Informationstechnik beträgt die Stellenzahl einschließlich Fachbereichsleitung 67,5 Stellen.

49. Welche Studiengänge werden an den Universitäten der Bundeswehr mit Bezug zur Cyberverteidigung angeboten (bitte Studiengänge nennen)?

a) Wie viele Studierende sind in diesen Studiengängen aktuell immatrikuliert (bitte nach Studiengängen aufschlüsseln)?

b) Wie haben sich die Neueinschreibungen seit Einführung dieser Studiengänge entwickelt (bitte nach Studiengängen aufschlüsseln)?

Die Fragen 49 bis 49b werden in nachfolgender Tabelle zusammen beantwortet:

Studiengang	Neuimmatrikulationen					Immatrikulierte Stand 1. Januar 2023
	2019	2020	2021	2022	2023	
Master-Studiengang Cybersicherheit (UniBw München)	18	29	29	37	49	86
Master-Studiengang Intelligence and Security Studies (UniBw München)	50 [davon haben die Vertiefung Cyber Defence gewählt: 11]	58 [Cyber Defence: 13]	69 [Cyber Defence: 14]	70	59	129

c) Werden in diesen Studiengängen Unterrichtsinhalte zur aktiven Cyberabwehr und aktiven Cyberabwehrmaßnahmen angeboten, und wenn ja, welche (bitte nach Modulen und angebotener Unterrichtsform aufschlüsseln)?

Folgende Module mit Unterrichtsinhalten zur aktiven Cyberabwehr und zu aktiven Cyberabwehrmaßnahmen werden an der Universität der Bundeswehr München angeboten:

Studiengang	Modul	Unterrichtsform
Cybersicherheit	Offensive Sicherheitsüberprüfungen bestehend aus:	
	Vorlesung Penetration Testing	Vorlesung
	Praktikum Penetration Testing	Praktikum
Cybersicherheit	Cyber Network Capabilities (CNC) Methoden bestehend aus:	
	Vorlesung CNC Methoden	Vorlesung
	Praktikum CNC Methoden	Praktikum

d) Wird in den Studiengängen mit dem KdoCIR kooperiert, und wenn ja, inwiefern?

Die Zusammenarbeit zwischen der UniBw M mit dem KdoCIR im Rahmen des Studiengangs Cybersicherheit erfolgt insbesondere bei der Durchführung von studentischen Abschlussarbeiten (Masterarbeiten), die in Kooperation mit und bei Einheiten aus dem Organisationsbereich CIR entstehen, sowie durch Gastvorträge akademisch gebildeten Personals des KdoCIR im Rahmen der von den Professuren gehaltenen universitären Lehre. Universität und KdoCIR tauschen sich zur Weiterentwicklung des Studiengangs Cybersicherheit miteinander aus, um eine Schärfung des Profils der Absolventinnen und Absolventen zu erreichen.

e) Wird in den Studiengängen mit dem BSI kooperiert, und wenn ja, inwiefern?

Die Zusammenarbeit zwischen der UniBw M mit dem BSI erfolgt in Forschungsprojekten sowie im Rahmen der Mitwirkung der UniBw M am NKCS; Ergebnisse dieser gemeinsamen Aktivitäten fließen in die forschungsnahen Lehrveranstaltungen im Studiengang Cybersicherheit ein.

50. Welche Lehrstühle und Professuren an den Universitäten der Bundeswehr beschäftigen sich in Lehre und Forschung mit aktiver Cyberabwehr?

    a) Wie sieht der zugehörige Lehrkörper für diese Lehrstühle und Professuren jeweils aus (bitte nach Besoldungsstufen aufschlüsseln)?

    b) Wie haben sich die Lehrkörper dieser Lehrstühle und Professuren seit ihrer Einrichtung entwickelt?

Die Fragen 50 bis 50b werden zusammen beantwortet.

Zum Lehrkörper an einer Universität gehören die Hochschullehrer und Hochschullehrerinnen (= Professoren und Professorinnen).

Im Jahr 2018 wurde an der Universität der Bundeswehr München die Professur „Datenschutz und Compliance“ eingerichtet. Die Professur ist mit der Besoldungsstufe W3 bewertet.

51. Wie viele finanzielle Mittel wurden durch die Bundeshaushalte für die Jahre 2020, 2021 und 2022 für Lehrstühle und Studiengänge mit Cybersicherheitsinhalten an Universitäten der Bundeswehr bereitgestellt, und wie viele Mittel werden 2023 und in der mittelfristigen Finanzplanung für 2024 und 2025 für Lehrstühle und Studiengänge mit Cybersicherheitsinhalten an Universitäten der Bundeswehr bereitgestellt?

Die nachstehende Tabelle gibt für die Universität der Bundeswehr München an, welche Mittel des Bundeshaushalts für Professuren und Studiengänge mit Cybersicherheits-Inhalten in den Jahren 2020 bis 2022 zur Verfügung standen und welche für die Jahre 2023 und 2024 geplant sind.

Mittel des Bundeshaushalts für Professuren und Studiengänge mit Cybersicherheits-Inhalten (Angaben in Mio. Euro)				
2020	2021	2022	2023 (Planung)	2024 (Planung)
10,4	10,4	10,6	11,7	11,7

52. Inwiefern gibt es Pläne seitens der Bundesregierung, die Universitäten der Bundeswehr zu zentralen Forschungsstellen für Cybersicherheit auszubauen?

Das Forschungsinstitut CODE der UniBw M wurde 2013 als universitätsinternes Forschungszentrum gegründet und ist 2017 zum ressorteigenen Forschungsinstitut „Cyber Defence und Smart Data“ (FI CODE) als zentrale wissenschaftliche Einrichtung der UniBw M aufgewachsen. In diesem Zuge wurden elf neue W3-Professuren geschaffen. Das FI CODE verfolgt das Ziel, technische Neuerungen, Innovationen und Konzepte zum Schutz von Daten, Software sowie IT-Systemen integrativ und interdisziplinär in einem universitären Umfeld zu erforschen und prototypisch zu entwickeln. Hierbei liegt der Fokus auf der Technologie-Entwicklung in den drei Themenfeldern Cyber Defence, Smart Data und Quantum Technology. Dazu bündelt das FI CODE wissenschaftliche Kompetenzen und arbeitet eng mit Partnern aus Bundeswehr, Behörden, Forschung und Wirtschaft zusammen. Die UniBw M soll so zu einem der zentralen Forschungs- und Entwicklungsorte für die IT-Sicherheitsforschung des Bundes ausgebaut werden (Cyber Cluster UniBw M) und die Kooperation mit einschlägigen Ressorts, anderen Sicherheitsbehörden des Bundes und der Länder, der Industrie und Wissenschaft sowie weiteren gesellschaftli-

chen Institutionen bei der Befassung mit Sicherheitstechnologien und Sicherheitsanwendungen ermöglichen.

53. Inwiefern gibt es Pläne seitens der Bundesregierung, die Universitäten der Bundeswehr zu zentralen Forschungsstellen für datengetriebene Krisenfrüherkennung auszubauen?

Die Universitäten der Bundeswehr dienen in erster Linie der wissenschaftlichen Ausbildung von Offizierinnen und Offizieren der Bundeswehr. An ihnen findet Grundlagenforschung und anwendungsbezogene Forschung zu verschiedenen Themen statt u. a. auch zu datengetriebener Krisenfrüherkennung. An der UniBw M wird hierzu insbesondere im Rahmen des Kompetenzzentrums Krisenfrüherkennung geforscht.

54. Inwiefern arbeitet die Bundeswehr mit dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) zusammen?

a) Mit welchen Abteilungen des FKIE arbeitet die Bundeswehr konkret zusammen?

b) Zu welchem Zweck arbeitet die Bundeswehr mit dem FKIE zusammen?

c) Inwiefern finden die Forschungsergebnisse der Abteilungen „Cyber Security“, „Cyber Analysis and Defense“ und „Kommunikationssysteme“ des FKIE Eingang in die Arbeit der Bundeswehr?

Die Frage 54 bis 54c werden zusammen beantwortet.

Das BMVg gewährt der Fraunhofer-Gesellschaft jährlich eine Zuwendung im Rahmen einer institutionellen Förderung gemäß § 44 der Bundeshaushaltsordnung. Aus diesen Fördermitteln ergibt sich für das FKIE eine (anteilige) Grundfinanzierung. Darüber hinaus fördert das BMVg einzelne Forschungsarbeiten im Rahmen von Projektzuwendungen. Diese Förderungen haben beim FKIE einen wesentlich geringeren Umfang als die Grundfinanzierung. Die geförderten Forschungsaktivitäten werden in den folgenden Abteilungen des Instituts erbracht:

- Abteilung Sensordaten- und Informationsfusion,
- Abteilung Informationstechnik für Führungssysteme,
- Abteilung Kommunikationssysteme,
- Abteilung Cyber Analysis und Defence,
- Abteilung Cyber Security,
- Abteilung Mensch-Maschine-Systeme,
- Abteilung Systemergonomie,
- Abteilung Kognitive Mobile Systeme.

Die grundfinanzierte Forschung dient dem Aufbau und dem Erhalt der Analyse- und Bewertungsfähigkeit und der Vorbereitung neuer Lösungsansätze zur Beantwortung von künftigen wehrtechnischen Fragestellungen. Es werden darüber hinaus neue wissenschaftliche Erkenntnisse und Technologien auf ihre wehrtechnische Relevanz hin untersucht.

Im Rahmen der angewandten Forschungsaktivitäten werden zukunftsweisende, als wehrtechnisch relevant erkannte Technologien aufgegriffen, näher analy-

siert und bei Bedarf mit Forschungsaktivitäten fortgeführt. Sie dienen dem Erhalt und dem Ausbau der wehrtechnischen Kompetenz in Deutschland.

Weitergehende Forschung dient der Analyse und dem Vorantreiben neuer Technologien bis hin zu ihrer Bewertung hinsichtlich der Anwendungsreife. Diese Aktivitäten sind auf die Erfüllung technologischer und systemtechnischer Anforderungen gemäß der zukünftig erforderlichen Fähigkeiten der Bundeswehr ausgerichtet und ermöglichen darüber hinaus, definierte Technologiebereiche über längere Zeiträume zu vertiefen bzw. hinsichtlich ihrer Technologiereife voranzutreiben.

Jedem grundfinanzierten Forschungsvorhaben des FKIE im Bereich Cyber- und Informationstechnologien aus den Abteilungen „Cyber Security“, „Cyber Analysis and Defence“ und „Kommunikationssysteme“ ist eine fachliche Ansprechperson aus dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) oder dem KdoCIR zugeordnet. Diese nehmen nicht nur die Forschungsergebnisse entgegen, sondern sind dazu auch in einem regelmäßigen fachlichen Austausch mit dem FKIE. Im KdoCIR fließen die Ergebnisse bspw. in die Fähigkeitsentwicklung der Streitkräfte mit ein, oder liefern im BAAINBw wissenschaftliche Impulse zur Lösung technologischer Herausforderungen bei der materiellen Bedarfsdeckung.

55. Plant die Bundesregierung, die Finanzmittel des FKIE aufzustocken, und wenn ja, in welcher Höhe, und wenn nein, warum nicht?

Der Pakt für Forschung und Innovation (PFI) sieht eine jährliche Steigerung der Zuwendungen an die Wissenschaftsorganisationen – auch an die Fraunhofer-Gesellschaft – in den Jahren 2021 bis 2030 um jeweils 3 Prozent vor.

56. Für welche Zwecke genau gibt die Bundesregierung dem FKIE Finanzmittel?

Im Bereich der Sensordaten- und Informationsfusion soll die Informationsverknüpfung verschiedener Sensor- und anderer Datenquellen erforscht und gesteigert werden.

Im Bereich der Informationstechnik für Führungssysteme werden Architekturen und Interoperabilitätslösungen für verteilte Führungsinformations- und Entscheidungsunterstützungssysteme erarbeitet. Im Bereich der Kommunikationssysteme werden konzeptionelle und experimentelle Forschungsarbeiten zur effizienten Nutzung, Aufklärung und Störung von Kommunikationssystemen vorgenommen.

Im Bereich Cyber Analysis & Defence wird der Schutz von IT-Systemen vor Cyberangriffen durch die Analyse verwundbarer Systeme, die Absicherung eigener Systeme sowie durch die Analyse von Cyberangriffen, Täterwerkzeugen und Akteuren erforscht.

Im Bereich Cyber Security wird Forschung zur Analyse von Angriffstechniken auf IT-Systeme sowie die Entwicklung von Ansätzen zu ihrer Erkennung und Abwehr durchgeführt.

Im Bereich Mensch-Maschine-Systeme wird erforscht, komplexe Technologien und Prozessabläufe für den Menschen eindeutig und transparent darzustellen und die Interaktionen von Mensch und Technik zeit- und stressrobust zu gestalten.

Im Bereich Systemergonomie werden nutzerzentrierte Ansätze weiterentwickelt und zusammen mit technologiefokussierten Perspektiven zu einem stim-

migen Zusammenspiel von Menschen, komplexen technischen Systemen und Prozessen zusammengebracht.

Im Bereich Kognitive Mobile Systeme werden wissenschaftliche Fragestellungen im Kontext der Führung von mobilen Ein- und Mehrrobotersystemen bearbeitet.

In der im Rahmen des PFI-geförderten Forschung liegt der Fokus auf Fragen der Digitalisierung in Bereichen der zivilen, der inneren bzw. der öffentlichen Sicherheit. Hinzu kommen vertiefte Erforschung und vertiefte forschungsnahe Entwicklung im Bereich der Cybersicherheit in Kritischen Infrastrukturen.

Besondere Bedeutung kommt Fragen der menschengerechten Digitalisierung erfolgskritischer Prozesse, der Erforschung effektiver und effizienter Mensch-Maschine-Systeme und ethischen Fragen im Bereich der Digitalisierung/Automatisierung zu.

57. Gibt es seitens der BMVg Pläne, Staaten wie Moldau, Georgien, die baltischen Staaten oder die Staaten des Westbalkans, mit IT-Hardware bzw. IT-Unterstützungsleistungen zu unterstützen, oder ist dies bereits geschehen?

Für die benannten Staaten ist im Sinne der Fragestellung derzeit nicht beabsichtigt, IT-Hardware bzw. IT-Unterstützungsleistungen bereitzustellen. Dies ist in der Vergangenheit auch nicht geschehen.

58. Gibt es seitens des BMVg Pläne, die Ukraine mit IT-Hardware bzw. IT-Unterstützungsleistungen zu unterstützen, oder ist dies bereits geschehen?

Es sind keine Lieferungen bzgl. IT-Hardware bzw. IT-Unterstützung an die Ukraine im Sinne der Fragestellung geplant oder bereits durchgeführt.

Ausgenommen hierbei sind Maßnahmen zur Softwarepflege und -änderung der Betriebssoftware sowie Austausch von Betriebshardware bereits gelieferter Systeme im Rahmen der logistischen Unterstützung.

59. Welche 25-Millionen-Euro-Vorlagen plant das BMVg, in den nächsten 36 Monaten im Zusammenhang mit der Beschaffung von Ausstattung für das KdoCIR und für Projekte der Digitalisierung der Bundeswehr dem Haushaltsausschuss vorzulegen (bitte quartalsweise aufschlüsseln)?

Das Verfahren zur Aufstellung des Bundeshaushalts 2024 hat erst begonnen. Hinsichtlich der geplanten 25-Mio.-Euro-Vorlagen im Jahr 2023 ist das Bundesministerium der Verteidigung bestrebt, Regierungshandeln transparent und nachvollziehbar zu gestalten. Entsprechend der etablierten Praxis werden daher der Haushaltsausschuss und der Verteidigungsausschuss des Deutschen Bundestages jeweils zu Beginn eines Jahres und nach der parlamentarischen Sommerpause über die in den Folgemonaten geplanten 25-Mio.-Euro-Vorlagen unterrichtet.

60. Welche rechtlichen Grundlagen sind aus Sicht des Bundesministeriums der Verteidigung für die Anwendung offensiver Cyberabwehrinstrumente für die Bundeswehr

a) derzeit einschlägig,

b) künftig, auch vor dem Hintergrund der vom Bundeskanzler ausgerufenen „Zeitenwende“, zusätzlich erforderlich?

Für den Einsatz militärischer Cyberfähigkeiten gelten dieselben völker- und verfassungsrechtlichen Rahmenbedingungen wie für den Einsatz anderer militärischer Fähigkeiten. Diese müssen im konkreten Einzelfall gegeben sein und bieten eine hinreichende Grundlage für die Erfüllung des verfassungsgemäßen Auftrags der Bundeswehr.

61. Welche aktiven Cyberabwehrmaßnahmen könnte die Bundeswehr derzeit technisch anwenden?

Im Bereich der Cyberverteidigung ist die Bundeswehr mit dem Zentrum Cyberoperationen befähigt, offensive und defensive Cyberoperationen durchzuführen. Hierzu verfügt sie über geeignete Fähigkeiten zur Aufklärung und Wirkung.

Auf die Antworten der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/10336 und auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/26855 wird verwiesen.

62. Welche aktiven Cyberabwehrmaßnahmen müssen aus Sicht des BMVg, auch vor dem Hintergrund der vom Bundeskanzler ausgerufenen „Zeitenwende“, künftig zusätzlich in das technische Fähigkeitsprofil der Bundeswehr aufgenommen werden?

Auf die Antwort zu Frage 3 wird verwiesen.

63. Welche Zusammenarbeit und welchen Austausch von Wissen in welcher Form (Angabe Anzahl deutsches Personal, Teilnahme an Übungen, Gesprächsformate) mit dem NATO COE Cyber Defence/Counter Intelligence gibt es?

Die mit den Begriffen „Cyber Defence“ und „Counter Intelligence“ verbundenen Themen sind der jeweilige Arbeitsgegenstand zweier unterschiedlicher „Centres of Excellence“ (COE) der NATO. Diese sind zum einen das „Cooperative Cyber Defence Centre of Excellence“ (CCD COE) in Tallin/EST, und zum anderen das „Counter Intelligence Centre of Excellence“ (CI COE) in Krakau/POL. Die COE sind nicht Teil der NATO-Kommando- und Streitkräftestruktur, aufgrund ihrer Akkreditierung aber Teil der Rechtskörperschaft der NATO.

Deutschland ist eine der Gründungsnationen des NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) und besetzt seit längerem drei Positionen (Chef des Stabes, Jurist, IT-Sicherheitsexperte).

Die Streitkräfte nehmen regelmäßig an beiden durch das CCD COE organisierten Cyber-Übungen (Locked Shields und Crossed Swords) teil, nutzen das angebotene Ausbildungs- und Weiterbildungsangebot, nehmen an diversen Gesprächsformaten teil (u. a. Cyber Commanders Forum, CyCon, projektbezogene Treffen) und beauftragen das COE wiederkehrend im Bedarfsfall.

Auf die Übungs- und Ausbildungsangebote des CCD COE wird auch durch Geschäftsbereichsbehörden des BMI zurückgegriffen.

Deutschland ist weiterhin Mitgliedsnation im NATO Counter Intelligence Centre of Excellence und entsendet Personal.

Der Fokus der Arbeit beim CI COE liegt in der Spionageabwehr in Operationen, Fortbildungen, Übungen, Regelungen, Konzepten und Strategien der NATO und Schaffung einer Institution für eine zentrale, standardisierte „Konservierung von Einsatzwissen“.

Die Betrachtung des Cyberraums im Bereich Spionageabwehr stellt hierbei lediglich ein Randthema dar. Eine grundlegende und fachspezifische Befassung mit dem Thema „Cyber- und Informationsraum“ findet am CI COE nicht statt.

64. Plant die Bundesregierung Änderungen im Vergaberecht bei Cyberabwehrmaßnahmen, um die Abschreckungsfähigkeiten Deutschlands zu erhöhen, und wenn ja, welche?

Seitens der Bundesregierung sind derzeit keine diesbezüglichen Änderungen im Vergaberecht geplant.

65. Plant die Bundesregierung Änderung der Arbeitszeitregelungen und Flexibilität der Beschäftigungsverhältnisse von Soldaten und Soldatinnen bzw. zivilen Mitarbeitern und Mitarbeiterinnen im Bereich der Cyberabwehr, und wenn ja, welche?

Es sind derzeit keine speziellen Änderungen im Sinne der Fragestellung geplant.

66. Plant die Bundesregierung die Auslagerung von Cyberabwehrfähigkeiten an externe Unternehmen und hierfür die rechtlichen Voraussetzungen zu schaffen?

Die Bundesregierung geht davon aus, dass hier mit dem Begriff „Cyberabwehrfähigkeiten“ ausschließlich staatliche Maßnahmen zur Abwehr von Gefahren im Cyberraum gemeint sind, die der Eingriffsverwaltung zuzuordnen sind. Derartige Maßnahmen bedürfen einer gesetzlichen Grundlage. Die Bundesregierung plant grundsätzlich nicht, derartige Maßnahmen an externe Unternehmen auszulagern.

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