Deutscher Bundestag **Drucksache 20/5070**

20. Wahlperiode 03.01.2023

Kleine Anfrage

der Fraktion der CDU/CSU

Verteidigung im Cyberraum – EU-Kooperation und aktive Cyberverteidigung

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 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.

Wir fragen daher die Bundesregierung:

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?
2. Welche Ableitungen trifft die Bundesregierung aus der Aufforderung der Europäischen Kommission an die Mitgliedstaaten, aktive Verteidigungskapazitäten im Cyberraum aufzubauen?
3. Welche aktiven Cyberfähigkeiten benötigt die Bundeswehr nach Ansicht der Bundesregierung in unmittelbarer und mittelbarer Zukunft?
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?
5. Was versteht die Bundesregierung unter sogenannten Hackbacks?
6. Was ist die Position des Bundesministeriums der Verteidigung (BMVg) bezüglich des Einsatzes sogenannter Hackbacks?
7. Inwiefern ist die militärische Cyberverteidigung Teil der in Erstellung befindlichen nationalen Sicherheitsstrategie?

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?

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?

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?

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

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?

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?

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?

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

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

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?

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

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?

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

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

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?

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?

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

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

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?

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)?
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)?
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?
31. Wer ist nach Kenntnis der Bundesregierung für die Verteidigung gegen Cyberangriffe auf Institutionen der EU zuständig?
32. Welche Form der Kooperation gibt es zwischen den „military Computer Emergency Response Teams“ der EU-Mitgliedstaaten?
33. Wieso beteiligt sich die Bundesregierung nicht am Projekt „Cyber Rapid Response Teams and Mutual Assistance in Cyber Security“ der Ständigen Strukturierten Zusammenarbeit?
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?
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?
36. Bewertet die Bundesregierung eine eigenständige deutsche und europäische Cybersicherheits- und Cyberverteidigungsbranche als notwendig, um die Landes- und Bündnisverteidigung auch im Cyberraum sicherzustellen?
37. Plant die Bundesregierung, Teile der Branchen Cybersicherheit und Cyberverteidigung als Schlüsseltechnologien zu definieren?
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)?
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?
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?
41. Gibt es konkrete Pläne einer Zusammenarbeit zwischen der Bundeswehr und Trägern ziviler kritischer Infrastruktur, etwa im Sinne eines Know-how-Transfers?

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?

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

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

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

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?

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

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

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)?

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

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

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

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?

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?

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

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

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?

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

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

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?

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

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)?

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?

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

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?

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?

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

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?

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

Berlin, den 21. Dezember 2022

Friedrich Merz, Alexander Dobrindt und Fraktion

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.bundesanzeiger-verlag.de
ISSN 0722-8333