Deutscher Bundestag **Drucksache 21/2835**

21. Wahlperiode 17.11.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Tobias Matthias Peterka, Andreas Paul, Ulrich von Zons, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/2420 –

Cybersicherheit und Personalzuwachs im Bereich IT-Sicherheit im Geschäftsbereich des Bundesministeriums der Verteidigung

Vorbemerkung der Fragesteller

Cybersicherheit ist ein zentrales Element moderner Verteidigungs- und Sicherheitspolitik. Angriffe auf IT-Infrastrukturen, Kommunikationssysteme und militärische Führungsfähigkeit stellen eine der größten Bedrohungen für die Handlungsfähigkeit von Staat und Streitkräften dar. Die Bundeswehr ist im Rahmen hybrider Bedrohungen zunehmend Ziel von Cyberoperationen staatlicher wie nichtstaatlicher Akteure (www.tagesschau.de/investigativ/ndr-wdr/cyberangriffe-bundeswehr-russland-100.html).

Die Schaffung zusätzlicher Stellen im Bereich Cyber- und IT-Sicherheit im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) ist daher von besonderer sicherheitspolitischer Bedeutung. Der Stellenzuwachs von rund 163 Stellen (www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/) verdeutlicht, dass das BMVg die Relevanz der Cyberabwehr erkannt hat und entsprechende Kapazitäten aufbaut.

Gleichzeitig hat die Bundesregierung im Bereich IT-Sicherheit Stellen abgebaut. Lediglich im militärischen Bereich gibt es einen Stellenzuwachs (s. o.).

Der Bundesrechnungshof hat vor eklatanten Sicherheitslücken in den Rechenzentren und Netzen des Bundes gewarnt (www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacfe5-2e6b-4e8b-a64b-e10d9cf2585e). Unter anderem bemängelt der Bundesrechnungshof, dass weniger als 10 Prozent der mehr als 100 Bundesrechenzentren die Mindeststandards erfüllen, dass die Notstromversorgung in Krisenlagen vielfach unzureichend ist und dass kritische IT-Dienste oft nicht georedundant verfügbar sind (s. o.).

Angesichts der von der ehemaligen Bundesregierung selbst als „besorgniserregend“ beschriebenen Cybersicherheitslage (www.security-insider.de/bund-reduziert-it-sicherheitsstellen-a-508f57e078fd32fa7cd1a915db00c76e/) stellt sich den Fragestellern u. a. die Frage nach den Gründen dieser Schwerpunktsetzung. Gleichzeitig stellen sich ihnen Fragen, wie die neuen Stellen im BMVg strategisch eingebunden, mit Kompetenzen ausgestattet und im internationalen Vergleich bewertet werden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 14. November 2025 übermittelt.

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

Vorbemerkung der Bundesregierung

Die Bundesregierung nimmt die Vorbemerkung der Fragesteller zur Kenntnis. Sie stimmt weder den darin enthaltenen Wertungen zu noch bestätigt sie die darin enthaltenen Feststellungen oder dargestellten Sachverhalte.

Cyberkriminelle und staatliche Akteure professionalisieren ihre Arbeitsweise. Sie sind technisch auf dem neuesten Stand und agieren aggressiv. Längst haben sie Strukturen für ihre kriminellen Dienstleistungen etabliert. Deutschland setzt der Bedrohung eine tragfähige Cybersicherheitsarchitektur entgegen. Diese Cybersicherheitsarchitektur muss unbedingt funktionsfähig bleiben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Sicherheitslage in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt (vgl. www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html).

Cyberbedrohungen gingen im vergangenen Jahr von diversen Angreifergruppen aus. Advanced Persistent Threats (APT)-Gruppen betrieben beispielsweise Cyberspionage und starteten Angriffe auf Behörden der auswärtigen Angelegenheiten, der Verteidigung und der öffentlichen Sicherheit und Ordnung. Auch Institutionen, die in diesen Bereichen tätig sind, waren betroffen. Darüber hinaus wurde die arbeitsteilige cyberkriminelle Schattenwirtschaft weiterhin professioneller. Sogenannte Access Broker handelten mit erbeuteten Zugangsdaten. Andere Cybercrime-Gruppen nutzten Zero-Day-Schwachstellen (d. h. Schwachstellen, die dem Hersteller noch nicht bekannt sind) zum Datendiebstahl.

Mit der weiter fortschreitenden Digitalisierung vergrößerten sich auch die Angriffsflächen im Bundesministerium der Verteidigung (BMVg). Über alle Arten von Cyberbedrohungen nehmen die Gefährdungen stetig weiter zu.

Von einem Ransomware-Angriff auf einen kommunalen IT-Dienstleister Ende Oktober 2023 waren beispielsweise 72 kommunale Kunden mit rund 20.000 kommunalen Arbeitsplätzen betroffen. Die Folge waren teils monatelange Ausfallzeiten.

Eine weitere Folge erfolgreicher Cyberangriffe sind exorbitante „Lösegeldzahlungen“ für durch Ransomware-Angriffe verschlüsselte Daten. Für gestohlene exfiltrierte Daten wurde dabei im Schnitt fast dreimal so viel gezahlt wie für erbeutete verschlüsselte Daten.

In allen Dimensionen hat sich die IT-Sicherheitslage deutlich verschärft: Zum einen führt der russische Angriffskrieg auf die Ukraine zu vermehrten Angriffen auf Verbündete der Ukraine (u. a. Deutschland) durch russlandfreundliche Cybergruppierungen oder mutmaßlich staatliche Stellen. Dabei müssen auch Sekundäreffekte zur Zerstörung von IT-Infrastruktur der Bundeswehr berücksichtigt werden.

Die stetig wachsende Komplexität der IT-Landschaft mit zunehmender Vernetzung von Behörden untereinander, mit Unternehmen, Bürgern sowie Cloud-Diensten erweitert die Wirkungsbreite von Angriffen auf einzelne Institutionen. Gleichzeitig erwartet die Bevölkerung zu Recht einen auch mit IT funktionierenden Rechtsstaat und resiliente Strukturen gegenüber Cyberangriffen in den Streitkräften sowie einen Fortschritt der Digitalisierung der öffentlichen Verwaltung.

Mit Blick auf die weiter fortschreitende Digitalisierung unserer Streitkräfte, sind angesichts der schnellen technologischen Entwicklung ständig Möglichkeiten zur Reduzierung der Gefährdungslage vorzuhalten. Im Bereich der Infor-

mationssicherheit in der Bundeswehr kommt der strategischen Vorausschau daher eine überragende Bedeutung zu.

Durch die Veröffentlichung sensibler Informationen wäre die in langjährigen Prozessen erarbeitete Resilienz der Informationstechnik des Geschäftsbereiches (GB) BMVg erheblich gefährdet.

Der Aufbau von Expertise, IT-Sicherheitsinfrastruktur, Prozessen und Resilienzfaktoren beansprucht umfangreiche Ressourcen und insbesondere Zeit. Der Wiederaufbau nach einem erfolgreichen Cyberangriff könnte aber einen solchen Schaden anrichten, dessen Behebung potentiell ein Vielfaches davon kosten würde.

Mit Blick auf die weiter fortschreitende Digitalisierung unserer Streitkräfte, sind angesichts der schnellen technologischen Entwicklung ständig Möglichkeiten zur Reduzierung der Gefährdungslage vorzuhalten. Dies bezieht sich besonders auf Anzahl, Ort und Ausstattung von Rechenzentren, Ergebnisse technischer Sicherheitsüberprüfungen, Anzahl registrierter Sicherheitsvorfälle oder Cyberangriffe, zugrundeliegende Bedrohungsanalysen, ergriffene und in Planung befindliche technische und organisatorische Maßnahmen gegen Cyberangriffe, Anzahl von Stellen in der IT-Sicherheit und deren Entwicklung sowie weitere Resilienzmaßnahmen wie Krisenstäbe sowie konkrete Angaben zu internationaler Kooperation und Krisenlagen. Im Bereich der Informationssicherheit in der Bundeswehr kommt der strategischen Vorausschau daher eine überragende Bedeutung zu.

Mit der Expertise des Chief Security Officer der Bundeswehr (CSOBw), dem Zentrum für Cybersicherheit der Bundeswehr sowie der Teilhabe am Cyber-Abwehrzentrum des BSI wird der oben dargestellten Gefährdungslage effektiv entgegengewirkt.

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, 161,193).

Das verfassungsmäßig verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird hier durch schutzwürdige Interessen von Verfassungsrang begrenzt, wozu auch und insbesondere Staatswohlerwägungen zählen. Konkrete Fragen zu Strukturen, Dienstposten, Aufgabenprofilen und Fähigkeiten, welche im Bundesministerium der Verteidigung mit dem Zweck der IT-Sicherheit bzw. Cyber-Abwehr aufgestellt wurden, können aus Gründen des Staatswohls nicht beantwortet werden.

Die Veröffentlichung solch detaillierter Informationen würde potenziellen Angreifern wertvolle Einblicke in die Ressourcen und Fähigkeiten im Bereich der IT-Sicherheit des Bundesministeriums der Verteidigung und der Bundeswehr gewähren. Dies würde die Wirksamkeit von Sicherheitsmaßnahmen untergraben und die Anfälligkeit der IT-Systeme des Bundesministeriums der Verteidigung erhöhen.

Genaue Angaben über Organisationsstrukturen, Personalstrukturen, Aufgabenbeschreibungen und Fähigkeitsentwicklungen unterfallen den Schutzbedürfnis-

sen der nationalen Sicherheit. Die Offenlegung würde es Angreifern ermöglichen, basierend auf der personellen Ausstattung in den Organisationsstrukturen und den dazugehörigen Aufgabenbeschreibungen und Fähigkeitsentwicklungen, Schutzniveau im Bereich der IT-Sicherheit und Cyberabwehr abzuleiten und ihre Angriffe effektiver planen zu können.

Eine Einstufung als Verschlusssache und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der IT-Sicherheit und Cyberabwehr und damit der Aufgabenerfüllung und Funktionsfähigkeit des genannten Ressorts nicht ausreichend Rechnung tragen. Schon die Angabe, wie das BMVg den Cybergefahren begegnet, welche Angriffe es erkannt hat, wie viele Personen welche IT-Sicherheitsaufgaben ausführen, welche Bedrohungsszenarien es betrachtet und welche internationalen Kooperationen bestehen oder nicht bestehen, könnte zu einer Analyse der Verwundbarkeiten und Änderung des Angriffsverhaltens führen, die eine weitere Abwehr der Cybergefahren unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich. Daher hält die Bundesregierung die Informationen der angefragten Art insbesondere vor der aktuellen Sicherheitslage und Bedrohungslage im Cyberraum für so sensibel, dass selbst ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

Daher können die Fragen 1, 2, 6, 8, 12, 13 nach sorgfältiger Prüfung und Abwägung nicht beantwortet werden.

1. Wie viele Stellen im Bereich IT-Sicherheit wurden seit 2022 im Geschäftsbereich des BMVg neu geschaffen (bitte nach Jahr, Behörde bzw. Dienststelle und Besoldungsgruppe aufschlüsseln)?

2. Welche Aufgabenprofile erfüllen die im Bereich IT-Sicherheit hinzugekommenen Stellen im BMVg (vgl. Frage 1, z. B. operative Cyberabwehr, Forschung und Entwicklung, Ausbildungsaufgaben, internationale Kooperationen)?

Die Fragen 1 und 2 werden zusammen beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

3. Wie werden die neuen Stellen (vgl. Frage 1) organisatorisch im BMVg und in der Bundeswehr (z. B. Cyber- und Informationsraum [CIR], Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr [BAAINBw], IT-Dienstleistungen) verortet?

Die Verteilung neuer Stellen auf die Dienststellen des GB BMVg orientiert sich grundsätzlich an Auftrag und Bedarf der jeweiligen Dienststellen.

4. Welche konkreten Gründe lagen der Entscheidung über den Stellenzuwachs im militärischen Bereich zugrunde, und welche operativen und strategischen Ziele werden mit dem Stellenzuwachs von rund 163 Stellen im Bereich Cyber- und IT-Sicherheit verfolgt (vgl. Vorbemerkung der Fragesteller)?

Die geänderte weltpolitische Lage hat eine konsequente Ausrichtung der Bundeswehr auf die steigende Bedrohungslage notwendig gemacht. Ziel ist es, den neuen Bedrohungsszenarien wirksam entgegen zu treten.

5. Inwiefern wurden bei der Entscheidung über den Stellenzuwachs im militärischen Bereich Bedrohungslagen wie staatlich gesteuerte Cyberangriffe, hybride Kriegsführung oder Angriffe auf kritische militärische Infrastrukturen berücksichtigt?

Es wird auf die Antwort zu den Fragen 3 und 4 verwiesen.

6. Wie viele Sicherheitsvorfälle oder Cyberangriffe wurden in den letzten fünf Jahren im Zuständigkeitsbereich des BMVg registriert, und wie wurde jeweils darauf reagiert (bitte nach Jahr, Anzahl der Zwischenfälle, Behörde und Art der Angriffe differenzieren)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

7. Welche Rolle spielt der CIR bei der Umsetzung des Personalzuwachses im IT-Sicherheitsbereich, und inwiefern wird die personelle Verstärkung im Bereich Cyber- und IT-Sicherheit mit der Gesamtstrategie des BMVg für den Cyber- und Informationsraum abgestimmt?

Die Gesamtstrategie des BMVg für den Cyber- und Informationsraum hat die Erhöhung der Resilienz und die Sicherstellung der Kriegstauglichkeit der Bundeswehr zum Ziel. Insoweit wird auch auf die Antwort zu Frage 4 verwiesen.

8. Wie hoch ist die aktuelle Zahl unbesetzter IT-Sicherheitsstellen im Geschäftsbereich des BMVg, und welche Maßnahmen ergreift die Bundesregierung, um diese Vakanzen zu schließen?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

9. Welche Ausbildungs- und Qualifikationsmaßnahmen setzt das BMVg ein, um die neu geschaffenen IT-Sicherheitsstellen mit geeigneten Fachkräften zu besetzen?

Fachkräfte werden an internen und externen Bildungseinrichtungen für ihre Aufgabe aus- und weitergebildet.

10. Welche Maßnahmen sind ggf. vorgesehen, um die Attraktivität und Wettbewerbsfähigkeit des BMVg auf dem Arbeitsmarkt für IT-Sicherheitsexperten zu gewährleisten?

Es wird auf die Antwort der Bundesregierung zu den Fragen 40 und 51 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/14270 verwiesen.

11. Welche Kooperationen mit Verbündeten (z. B. NATO, EU) bestehen im Bereich Cyberabwehr, und inwiefern sind die zusätzlichen Stellen im BMVg für die Erfüllung dieser internationalen Verpflichtungen vorgesehen?

Es gibt eine Vielzahl von Kooperationen mit Verbündeten im Sinne der Fragestellung, unter anderem über das NATO Cyber Operations Centre und die NATO Malware Information Sharing Plattform. Ergänzend wird auf die Antwort der Bundesregierung zu den Fragen 16 und 19 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/5597 verwiesen. Im Bundesministerium der Verteidigung werden keine zusätzlichen Stellen für die Kooperation mit Verbündeten geschaffen.

12. Wie wird durch die Stellenmehrung sichergestellt, dass die Bundeswehr in multilateralen Strukturen (NATO, EU, bilaterale Partnerschaften) ihre Rolle als verlässlicher Partner im Bereich Cyber- und Informationsraum stärken kann?

13. Welche konkreten Auswirkungen erwartet die Bundesregierung durch den Stellenzuwachs (vgl. Vorbemerkung der Fragesteller) auf die Fähigkeit der Bundeswehr, Cyberangriffe abzuwehren und offensive sowie defensive Cyberoperationen durchzuführen?

Die Fragen 12 und 13 werden zusammen beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

14. Welche Bedeutung misst die Bundesregierung der personellen Verstärkung im BMVg (vgl. Vorbemerkung der Fragesteller) für die gesamtstaatliche Cybersicherheitsarchitektur bei, und wie wird eine Verzahnung mit anderen Ressorts und Behörden (z. B. BSI, Bundesministerium des Innern [BMI], Auswärtiges Amt) sichergestellt?

Die personelle Verstärkung im Sinne der Fragestellung hat eine hohe Bedeutung für die gesamtstaatliche Cybersicherheitsarchitektur. Die zuständigen Behörden führen regelmäßig strategische Lagebesprechungen durch und nutzen das National Cyber Abwehrzentrum, um einen operativen und technischen Informationsaustausch zu gewährleisten.

15. Wie bewertet die Bundesregierung die strategische Bedeutung der Cybersicherheit im Geschäftsbereich des BMVg für die Verteidigungsfähigkeit Deutschlands?

Es wird auf die Vorbemerkung der Bundesregierung in ihrer Antwort auf die Kleine Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/5597 verwiesen.

16. Plant die Bundesregierung, die gewonnenen Erkenntnisse und die Strukturen aus dem militärischen Bereich auch für den zivilen Bereich nutzbar zu machen, um den dortigen Kapazitätsabbau auszugleichen?

Die Bundesregierung plant, die im militärischen Bereich gewonnenen Erkenntnisse und Strukturen auch für den zivilen Bereich der Cybersicherheit nutzbar zu machen, um die Resilienz kritischer Infrastrukturen zu stärken. Dies ist ein zentrales Element der aktuellen Cybersicherheitsstrategie. Ergänzend wird auf die Antwort der Bundesregierung zu Frage 12 der Kleinen Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/14270 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.bundesanzeiger-verlag.de
ISSN 0722-8333