

Kleine Anfrage

der Abgeordneten Tobias Matthias Peterka, Andreas Paul, Ulrich von Zons, Lukas Rehm, Manfred Schiller, Tobias Teich, Gerold Otten, Dr. Rainer Kraft, Jan Wenzel Schmidt, Thomas Korell, Dr. Paul Schmidt, Robin Jünger, Dr. Malte Kaufmann, Dr. Daniel Zerbin, Dr. Christina Baum, Mirco Hanker, Reinhard Mixl, Marc Bernhard, Dr. Michael Blos, Carolin Bachmann, Stefan Keuter, Knuth Meyer-Soltau, Claudia Weiss, Julian Schmidt, Dr. Maximilian Krah, Achim Köhler, Edgar Naujok, Kay-Uwe Ziegler, Joachim Bloch, Udo Theodor Hemmelgarn, Stefan Henze, Uwe Schulz, Sascha Lensing, Rocco Kever, Volker Scheurell, Otto Strauß, Tobias Ebenberger und der Fraktion der AfD

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

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 strate-

gisch eingebunden, mit Kompetenzen ausgestattet und im internationalen Vergleich bewertet werden.

Wir fragen die Bundesregierung:

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)?
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?
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)?
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?
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)?
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?
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?
9. Welche Ausbildungs- und Qualifikationsmaßnahmen setzt das BMVg ein, um die neu geschaffenen IT-Sicherheitsstellen mit geeigneten Fachkräften zu besetzen?
10. Welche Maßnahmen sind ggf. vorgesehen, um die Attraktivität und Wettbewerbsfähigkeit des BMVg auf dem Arbeitsmarkt für IT-Sicherheitsexperten zu gewährleisten?
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?
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?
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?
15. Wie bewertet die Bundesregierung die strategische Bedeutung der Cybersicherheit im Geschäftsbereich des BMVg für die Verteidigungsfähigkeit Deutschlands?
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?

Berlin, den 22. Oktober 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

