Deutscher Bundestag **Drucksache 19/22268**

19. Wahlperiode 10.09.2020

Kleine Anfrage

der Abgeordneten Christian Sauter, Alexander Graf Lambsdorff, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Hartmut Ebbing, Dr. Marcus Faber, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Manuel Höferlin, Reinhard Houben, Olaf in der Beek, Dr. Christian Jung, Karsten Klein, Dr. Marcel Klinge, Pascal Kober, Oliver Luksic, Alexander Müller, Frank Müller-Rosentritt, Bernd Reuther, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Dr. Hermann Otto Solms, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Gerald Ullrich und der Fraktion der FDP

Aufstellung der Cyber-Reserve der Deutschen Bundeswehr

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

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

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

Nichtsdestotrotz sind aus Sicht der Fragesteller wesentliche Fragen im Zusammenhang mit der Gewinnung und Einsetzung der Cyber-Reservisten ungeklärt. Der bestehende Mangel an Fach- und Einsatzpersonal, Materialien und der Finanzierung der Bundeswehr sind durchaus öffentlich bekannt. Aufgrund der steigenden Zahl an IT-Angriffen auf staatliche und zivile Infrastrukturen kann die Bundesregierung nicht ohne wesentliche strukturelle und organisatorische Veränderungen im Aufbau der Cyber-Reserve das neue Jahrzehnt bestreiten. Zum Ausgleich des Personalmangels müssen neue Wege gegangen und verkrustete Strukturen aufgebrochen werden.

Wir fragen die Bundesregierung:

1. Welche Bedeutung hat Cyber-Sicherheit und besonders eine funktionierende Cyber-Reserve für die Verteidigungsfähigkeit Deutschlands im Cyber-Raum?
2. Seit wann wurde am Konzept einer Cyber-Reserve gearbeitet, welche Meilensteine markieren den Weg der Entwicklung bis zur Aufstellung, und welche sind bis 2030 geplant?
3. Welche in- sowie ausländischen staatlichen und nichtstaatlichen Akteure bedrohen aus Sicht der Bundesregierung die Cyber-Sicherheit der Bundesrepublik Deutschland (bitte detailliert begründen)*?*
4. Wie bewertet die Bundesregierung die Äußerungen des Inspekteurs CIR, Generalleutnant Ludwig Leinhos, der sich in einem Interview mit dem rechtlich zulässigen Einsatz der Bundeswehr im Inland und besonders mit der Steigerung der Reaktionsfähigkeit auf Cyber-Angriffe auseinandersetzt (Quellen: https://www.faz.net/aktuell/politik/inland/cyberabwehr-verteidigungsfaelle-bitte-nur-werktags-von-9-bis-17-uhr-16311910.html; https://augengeradeaus.net/2019/06/bundeswehr-plaediert-fuer-digitalen-verteidigungsfall-zur-besseren-cyber-abwehr/)?
   a) Welche Rolle spielt die Cyber-Reserve in diesem Kontext?
   b) Ist eine Änderung der rechtlichen Grundlage für den Einsatz der Cyber-Reserve in einem „digitalen Verteidigungsfall“ geplant, um schneller auf Cyber-Angriffe reagieren zu können?
   c) Warum gibt es, wie von Generalleutnant Ludwig Leinhos angeregt, keine Koordinierungsstelle, die den reibungslosen Übergang von Cyber-Abwehr zu Cyber-Verteidigung sicherstellt?
   d) Wie weit ist der Planungsstand des sogenannten Cyberabwehrzentrums Plus“, und wann soll es seine Tätigkeit vollumfänglich aufnehmen?
   e) Anhand welcher Kriterien stellt die Bundesregierung fest, ob ein Cyber-Angriff in die Zuständigkeit der Polizei bzw. der Nachrichtendienste fällt?
5. Wie weit ist der Aufbau der Cyber-Reserve fortgeschritten?
   a) Wie viele Dienstposten sind eingeplant, und wie viele sind derzeit besetzt (bitte jeweils in Dienstgrad und Laufbahn aufschlüsseln)?
   b) Wie hoch ist der Frauenanteil bei den besetzten Dienstposten, und welchen Prozentsatz hat sich die Bundesregierung als Ziel gesetzt?
   c) Welche Maßnahmen ergreift die Bundesregierung zur Personalgewinnung?

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

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

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

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

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

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

7. Was beinhaltet die Ausbildung der Cyber-Reservisten?

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

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

Falls ja, welche, und was beinhalten sie?

Falls nein, warum nicht?

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

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

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

b) Falls nein, warum nicht?

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

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

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

a) Falls ja, wie?

b) Falls nein, warum nicht?

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

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

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

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

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

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

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

Berlin, den 26. August 2020

Christian Lindner 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.betrifft-gesetze.de
ISSN 0722-8333