2766/J XXVI. GP

Eingelangt am 30.01.2019

ANFRAGE

der Abgeordneten **Rudolf Plessl** und GenossInnen

an den **Bundesminister für Landesverteidigung**

betreffend ***Abwertung der Cyber-Defence durch Reorganisation im BMLV***

Das Österreichische Bundesheer wird auf Wunsch der Ressortleitung aktuell wieder einmal umstrukturiert. Dies hat zur Folge, dass auch der weitere Aufbau des erst kurz zuvor aufgestellten Kommandos Führungsunterstützung & Cyber Defence – vermutlich auf Grund budgetärer Engpässe – wieder gestoppt wurde und neu strukturiert wird.

Auf Grund der aktuellen Bedrohungslage und wahrscheinlicher Bedrohungsszenarien gibt es international klare Entwicklungen auf die individuellen nationalen und gemeinschaftlichen militärischen Bedürfnisse abgestimmte Strukturen für Einsätze im Cyberraum vorzuhalten. Als Reaktion wird in zahlreichen Streitkräften das Spezialgebiet „Cyber“ entsprechend aufgewertet und ausgebaut. Auch für Österreich wäre es wichtig, sowohl gesamtstaatlich als auch speziell im militärischen Bereich entsprechende Cyber-Fähigkeiten nachhaltig und skalierbar zu verankern. Stattdessen wird im Zuge der neuen Heeresgliederung das bereits dafür zuständige Kommando Führungsunterstützung und Cyber Defence wieder aufgelöst und andere nachgeordnete Abteilungen in unterschiedlichste Strukturen „verräumt“ – **statt einer Konzentration beschränkter Kräfte und Ressourcen werden diese absichtlich zersplittert und abgewertet!**

Dadurch kommt es bei den militärischen Cyber-Kapazitäten jedoch zu einer äußerst nachteiligen Entwicklung im gesamten Bundesheer. Die nachhaltige Schwächung des „Cyber Defence“-Bereichs im BMLV geht jedoch interessanterweise mit einer signifikanten Stärkung des „Cyber Security“-Bereichs im BMI einher. Weiters soll der angekündigte Aufbau eines eigenen Nationalen Cyber Sicherheitszentrums (laut Regierungsprogramm) in der Stiftskaserne wohl der Öffentlichkeit „vortäuschen“, dass damit auch die militärische Verantwortung für den Cyber-Bereich gestärkt wird – **Dies ist ausgehend von den aktuellen Maßnahmen aber SICHER NICHT der Fall!**

Daher richten die unterfertigten Abgeordneten an den Bundesminister für Landesverteidigung nachstehende

Anfrage:

1. „Ein Europa das schützt“, war das Motto der Österreichischen EU-Ratspräsidentschaft. Welche Akzente setzte und setzt das BMLV zur nachhaltigen Verankerung und dem nachhaltigen, skalierbaren Aufbau eines militärischen „Cyber Defence“-Bereichs im Rahmen der Neuorganisation des Bundesheers?
    a. *Ist eine Kooperation mit europäischen Partnern vorgesehen und möglich?*
    b. *Wenn JA, mit welchen Staaten soll bzw. wird bereits kooperiert?*
    c. *Wenn NEIN, warum nicht?*

2. Welche Schlussfolgerungen ergeben sich für das Österreichische Bundesheer aus der neuen „Österreichischen Cyber Sicherheitsstrategie“ (ÖSCS2.0) betreffend militärische Cyberverteidigung?

3. Soll im Bereich Landesverteidigung eine eigene Cyber Verteidigungsstrategie, die die Aufgaben und Zielsetzungen im Bereich der Cyber Verteidigung klar regelt und strategische Ziele festlegt, realisiert werden?
    a. *Wenn JA, wie ist der aktuell Stand dieser Cyber-Verteidigungsstrategie?*
    b. *Wenn JA, wann soll diese in Kraft treten und umgesetzt werden?*
    c. *Wenn JA, auf welchen strategischen, fachlichen und operativen Grundlagen wird bei der Erstellung aufgebaut?*
    d. *Falls NEIN, warum nicht?*

4. Die Bedeutung Hybrider Einsätze oder Cyberbedrohungen als wahrscheinlichste neue Bedrohungsszenarien wird inzwischen häufig angesprochen. Liegen den aktuellen Umstrukturierungen im ÖBH daher konkrete Konzepte und Grundlagen zur Berücksichtigung sich wandelnder Bedrohungsszenarien zugrunde?
    a. *Welcher Prioritätensetzung folgen Sie, um im Bereich Cyber-Security/-Defence entsprechende Vorsorgemaßnahmen zu setzen und Einsatzkompetenzen bereit zu halten?*
    b. *Wurden bereits Schwerpunkte für den militärischen Cyber-Bereich verbindlich festgelegt?*
    c. *Wenn NEIN, warum nicht?*

5. Was sind die konkreten Gründe die Restrukturierung des ÖBH so vorzunehmen, dass die bestehenden Cyber-Kräfte zersplittert statt gestärkt werden?

6. Was sind die fachlich ausschlaggebenden Gründe für das BMLV, die geplanten Re-dimensionierungs- und Reorganisationsmaßnahmen mit vollkommen zersplitterten Zuständigkeits- und Kommandostrukturen umzusetzen?

   a. *Bleibt durch die vorgesehenen Strukturen der Grundsatz klarer Führungsverhältnisse und rasche Entscheidungsfindungen in diesem sensiblen Bereich weiterhin sichergestellt?*
   b. *Welche Vorteile soll die vorgesehene Kommando- und Organisationsstruktur, die sich künftig über mehrere unterschiedliche Kommando- und Verantwortungsbereiche mit jeweils verteilten Aufgabenstellungen erstreckt, erzielen?*

7. Entsprechen Ihre Umsetzungsvorgaben als Ressortchef den strategischen und militärischen Vorschlägen des Generalstabs?
   a. *Welche Experten aus dem Generalstab waren in die Erarbeitung der Grundlagen für die aktuellen Restrukturierungsmaßnahmen eingebunden?*
   b. *Welche internationalen Standards und „Best practice"-Vorbildern aus dem Bereich Cyber Defence folgen die von Ihnen gesetzten Restrukturierungsmaßnahmen?*
   c. *Gab es von Seiten des Generalstabes auch andere Reorganisationsvorschläge für den Bereich Cyber Defence im ÖBH? Wenn JA, warum wurden diese Vorschläge von Ihnen nicht umgesetzt?*

8. Warum wird das neue IKT&Cyber-Sicherheitszentrum nicht unmittelbar dem Generalstab nachgeordnet?
   a. *Welche militärisch-fachliche Begründung besteht dafür, das IKT- & Cyber-Sicherheitszentrum und die Führungsunterstützungsschule in die Streitkräftebasis einzugliedern?*
   b. *Warum werden diese Einheiten nicht der Einsatzorganisation in den Streitkräften zugeordnet?*

9. Welche Mehrwert für das Österreichische Bundesheer im Bereich Cyber-Fähigkeiten sehen Sie als Ressortchef in der Umsetzung der geplanten Restrukturierungmaßnahmen?

10. Erwarten Sie eine Steigerung oder Reduktion der Cyber-Fähigkeiten des ÖBH…
    a. *...im täglichen Betrieb?*
    b. *...im Cyberkrisenfall?*
    c. *...im Cyberverteidigungsfall?*

11. Ist sichergestellt, dass für das neue „IKT- & Cyber-Sicherheitszentrum" ausreichend Budgetmittel verfügbar bleiben?

12. Wie stellen Sie als verantwortlicher Ressortminister sicher, dass beim neuen IKT- & Cyber-Sicherheitszentrums die bisherige Qualität beibehalten und ausgebaut wird und drohenden Abwanderungstendenzen von MitarbeiterInnen aus dem Bereich der Cyber-Landesverteidigung in andere Ressorts (z.B. BMI) oder in die Privatwirtschaft erfolgreich begegnet und aktiv entgegengewirkt wird?

13. Ist vorgesehen, dass der Bereich der IKT-Sicherheit - losgelöst von allen anderen verantwortlichen Stellen – künftig durch das Abwehramt wahrgenommen werden soll?
    a. Wenn JA, welche fachlichen Grundlagen sprechen dafür?
    b. Wenn NEIN, welche fachlichen Gründe sprechen für eine andere Organisationsform?

14. Ist weiterhin vorgesehen, im Abwehramt jener Fähigkeiten zu bündeln die notwendig sind, um die Rolle als „Cyber Verteidigungszentrums“ (CVZ) wahrnehmen zu können?

15. Welche Aufgaben soll der Cyberverteidigungsbereich (Cyber Defence) künftig im Österreichischen Bundesheer – in Hinblick auf die gegenwärtigen und zukünftigen militärischen Herausforderungen – übernehmen und bewältigen können?

16. Ist vorgesehen, die budgetären Mittel für den militärischen Cyberbereich…
    a. ...schrittweise in den kommenden Jahren zu erhöhen?
    b. ... schrittweise, von den bisher vorgesehenen Budgetplanungen für die Jahre 2019-2022 zu kürzen?
    c. Falls Steigerungen/ Kürzungen vorgesehen sind, welche Bereiche sind jeweils konkret von diesen betroffen?

17. Ist vorgesehen, die personellen Ressourcen für den militärischen Cyberbereich…
    a. ...in den kommenden Jahren zu erhöhen?
    b. ... jedenfalls beizubehalten?
    c. ...zu reduzieren?

18. Welche Schwerpunkte setzten und planen Sie…
    a. ...beim Aufbau und der Implementierung einer effizienten militärischen Cyber-Verteidigung?
    b. ...im Bereich der elektronischen Drohnenabwehr?

19. Wann wird das „Leuchtturmprojekt Nationales Cyber Sicherheitszentrum“ in der Stiftskaserne tatsächlich gestartet?
    a. Welche(s) Ressort(s) übernimmt/-nehmen hier jeweils die Führungsrolle im Planungsstadium, in der Realisierung und dann im tatsächlichen Betrieb?
    b. Welche Ressorts sind in das Projekt bisher eingebunden?
    c. Welcher Umsetzungszeitrahmen ist für diese Projekt vorgesehen?
    d. Welche budgetären Kosten sind für diese Projekt vorgesehen und wie gestaltet sich der Finanzierungsschlüssel für die teilnehmenden Ressorts?