5034/J
vom 20.01.2021 (XXVII. GP)
ANFRAGE

der Abgeordneten Robert Laimer,

Genossinnen und Genossen,

an die Bundesministerin für Landesverteidigung

betreffend **konsequenter Verschleppung dringend notwendiger Maßnahmen zur Weiterentwicklung einer leistungsfähigen Cyberverteidigung des Österreichischen Bundesheeres.**

Vor fast fünf Jahre wurden im Landesverteidigungsministerium die dringlich notwendigen militärischen Vorarbeiten zu einem eigenen „Kommando Führungsunterstützung und Cyber Defence", begonnen.

Damals war jedem Verantwortlichen klar, dass vieles notwendig ist. Heute steht das Bundesheer nahezu wieder am Anfang seiner Anstrengungen. Laufend geänderte Bedrohungsszenarien und Eintrittswahrscheinlichkeiten, Reform über Reform, stets neue Strukturen – nur die notwendigen Fähigkeiten im Cyberverteidigungsbereich wurden nicht aufgebaut.

Anfang des Jahres 2020 wurde bei der Abwehr des Cyberangriffs auf das Außenministerium, auch auf die Expertise und Unterstützung der Cyberverteidigungs-Kapazitäten des Verteidigungsressorts zurückgegriffen. Nur in einer gemeinsamen Kraftanstrengung, konnte diese Bedrohung im Außenministerium in den Griff bekommen werden.

Resümee: In Österreich sind die zuständigen Stellen für die „Cybersicherheit" und für die „Cyberverteidigung", schon bei einem etwas größeren Angriff nicht mehr in der Lage, eigenständig ihren Aufgabenumfang zu bewältigen.

Das Bundesheer wurde dabei nach dem Grundsatz „Helfen, wo andere nicht mehr können", zu einem Assistenzeinsatz zur Cyberabwehr angefordert. Dabei wurden Cyberexperten des Verteidigungsressorts für eine mehrwöchige Unterstützungsleistung ins BMEIA abgestellt. Damit wurde die Aufrechterhaltung des Schutzes der eigenen militärischen Systeme im Bundesheer massiv gefährdet, da die ohnehin personell mager ausgestatteten Cyberkräfte des Bundesheeres an ihre Leistungsgrenze gebracht wurden.

Die Cyberkräfte des Bundesheeres sind bereits seit Jahren finanziell, strukturell und personell unterdotiert, sie wurden mehrfach umstrukturiert, zusammengekürzt, aber nicht für künftige Herausforderungen und Aufgabenstellungen, weiterentwickelt.

Parlamentarische Anfragen der letzten Jahre brachten bisher keinerlei Aufklärung. Entweder wurde bei den Beantwortungen,

- auf die militärische Geheimhaltung verwiesen und damit einer konkreten Beantwortung ausgewichen,
- eine Absicht hingewiesen, die bis heute nicht umgesetzt wurde,
- etwas angekündigt, dass noch nicht realisiert werden konnte,
- oder auf laufende Bearbeitungen hingewiesen, die nun schon über Jahre erfolgen.

Faktum ist, dass der Fähigkeitsbereich Cyberverteidigung im Bundesheer dringend aufgestellt werden muss, damit er den gegenwärtigen Herausforderungen und künftigen Aufgabenstellungen entsprechen kann. Dies gilt in gleicher Weise für die kernmilitärischen Aufgabenstellungen im Norm-, Übungs- und Einsatzbetrieb, als auch für die gesamtstaatliche Beitragsleistung im Sinn von Amtshilfen oder Assistenzleistungen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Hybride- oder Cyberbedrohungen gelten auch als wahrscheinlichste neue Bedrohungsszenarien. Liegen den aktuellen Umstrukturierungsabsichten im ÖBH konkrete Konzepte und Grundlagen zur Berücksichtigung der sich wandelnder Bedrohungsszenarien zugrunde?

2. Auf gesamtstaatlicher Ebene steht die „Österreichische Cyber Sicherheitsstrategie 2.0" (ÖSCS) kurz vor der Finalisierung. Auch in ihrem Ressort wurden jahrelang intensive Bearbeitungen zu Cyber-relevanten Strategien und Konzepten getätigt. Wann wird im BMLV eine Strategie zur militärischen Cyberverteidigung (Cyber Defence) verfügt?

3. Seit 2016 wird in ihrem Ressort der Fähigkeitsbereich Cyberverteidigung beurteilt und geplant. Wann werden im BMLV die einzelnen Cyberverteidigungskonzepte und Fähigkeitskataloge für den Fähigkeitsbereich Cyberverteidigung verfügt?

4. Sind die entsprechenden Vorhaben- und Realisierungsplanungen für eine merkliche Weiterentwicklung des Cyberverteidigungsbereichs bereits auf Schiene?

5. Werden die budgetären Mittel für den militärischen Cyberbereich in den nächsten Jahren erhöht, gleich belassen oder gekürzt?

6. Werden die budgetären Mittel für personellen Ressourcen im militärischen Cyberbereich in den nächsten Jahren erhöht, gleich belassen oder gekürzt?

7. Werden die die materiellen Ressourcen für den militärischen Cyberbereich in den nächsten Jahren gleich belassen, ausgebaut oder reduziert?

8. Werden die infrastrukturellen Ressourcen für den militärischen Cyberbereich in den nächsten Jahren gleich belassen, ausgebaut oder reduziert?

9. In den Budgetberatungen wurde festgehalten, dass für die Finanzjahre 2021 und 2022 zusätzlich jeweils 20 Mio. Euro für den Cyberverteidigungsbereich zur Verfügung gestellt werden. Sind damit aus militärischer Sicht wirkliche fähigkeitsverbessernde Maßnahmen zu erreichen?

10. Was genau wird mit den insgesamt 40 Millionen Euro finanziert? Wieviel davon wird hier für das Personal, wieviel für Ausstattung und wieviel für Infrastruktur aufgewendet?

11. Welche Schwerpunkte werden sie 2021 im Bereich „Cyber Intelligence" (nachrichtendienstliche Cyber Abwehr) setzen?

12. Welche Schwerpunkte werden sie 2021 im Bereich „CIS-Defence“ (IKT-Sicherheit) setzen?

13. Welche Schwerpunkte werden sie 2021 im Bereich „Cyber Operations“ (operative Cyber Abwehr) setzen?

14. Erwarten Sie in der laufenden Legislaturperiode eine Steigerung oder Reduktion der Cyber-Fähigkeiten des ÖBH
    - im Tagesbetrieb/Normbetrieb?
    - im Cyberkrisenfall?
    - im Cyberverteidigungsfall?
    - bis wann?

15. Sie haben Mitte letzten Jahres angekündigt, das IKT & Cybersicherheitszentrum dem Generalstab unmittelbar zu unterstellen. Wann wird das konkret erfolgen?

16. Wann bekommen das Abwehramt, das Heeresnachrichtenamt und das IKT & Cybersicherheitszentrum, entsprechenden Organisationspläne und Planstellen, um ihre Aufgaben im Cyberbereich wahrnehmen zu können?

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

18. Wie stellen Sie als verantwortliche Ressortministerin sicher, dass beim IKT- & Cyber-Sicherheitszentrums die bisherige Qualität beibehalten und ausgebaut wird und den bereits in einem hohen Maße erfolgten 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?

19. Die Cyberkräfte werden in den Waffengattungen Cybertruppe, EloKa-Truppe (Elektronische Kampfführung), IKT-Truppe und im MilGeoWesen weiterentwickelt. Wo setzen sie dabei die Schwerpunkte?

20. Die Domäne Cyber und die Domäne Information werden derzeit im BMLV getrennt betrachtet. Werden sie diese Domänen hinkünftig zusammenführen?

21. Welchen Mehrwert für das Österreichische Bundesheer im Bereich Cyber-Fähigkeiten sehen Sie als Ressortchefin in der Umsetzung der neuen geplanten Organisation?

Sollte eine detaillierte Beantwortung einzelner Fragen aus Geheimhaltungsgründen nicht möglich sein, so wird dennoch um eine Beantwortung mit möglichst hohem Informationsgehalt im Sinne des parlamentarischen Interpellationsrechts ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über Informationsordnung des Nationalrates und des Bundesrates – InfOG.

(SILVAN)

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-01-20T13:58:14+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	