MAG. KLAUDIA TANNER
BUNDESMINISTERIN FÜR LANDESVERTEIDIGUNG

S91143/15-PMVD/2021 19. März 2021

Herrn
Präsidenten des Nationalrates

Parlament
1017 Wien

Die Abgeordneten zum Nationalrat Laimer, Genossinnen und Genossen haben am 20. Jänner 2021 unter der Nr. 5034/J an mich eine schriftliche parlamentarische Anfrage betreffend „konsequente Verschleppung dringend notwendiger Maßnahmen zur Weiterentwicklung einer leistungsfähigen Cyberverteidigung des Österreichischen Bundesheeres“ gerichtet. Diese Anfrage beantworte ich wie folgt:

Zu 1:

Die Planungen zur Implementierung von Fähigkeiten der Cyber-Sicherheit und Cyber-Verteidigung werden von den Planungszielen des militärstrategischen Konzepts abgeleitet, welche zuletzt mit 27. November 2020 aktualisiert wurden und mit einem prognostizierten Risikobild 2030 hinterlegt sind.

Zu 2 und 3:

Die Bearbeitungen der „Österreichischen Cyber Sicherheitsstrategie 2.0 (ÖSCS 2.0)“ sind derzeit nicht finalisiert und unterliegen der interministeriellen Abstimmung. Daher können die Auswirkungen dieser Strategie auf das Bundesministerium für Landesverteidigung (BMLV), wie auch eine ressortinterne Strategie zur Cyber-Verteidigung, die eine weitere Abstimmung mit anderen Ressorts erfordert, nicht abschließend beurteilt werden. Der Entwurf eines Fähigkeitenkatalogs der Cyber-Truppe wurde bereits im März 2020 erstellt. Weitere Bearbeitungen erfolgen im Rahmen der Projektorganisation „UNSER HEER“.

Zu 4, 5 und 7 bis 10:

Zur Realisierung von Vorhaben der Cyber-Sicherheit sind mehrere Planungsvorgänge gleichzeitig in Bearbeitung, die in den Jahren 2021 und 2022 mit Hilfe des Sonderinvestitionspakets „Cyber-Sicherheit“ umgesetzt werden sollen. Mit den zur Verfügung

stehenden Volumina von 40 Mio. Euro sind selbstverständlich fähigkeitsverbessernde Maßnahmen, die auch den infrastrukturellen Bereich betreffen, erreichbar. Konkret sind im Rahmen des Sonderinvestitionspakets „Cyber-Sicherheit“ 33,4 Mio. Euro für Ausrüstung und Ausstattung sowie 6,6 Mio. Euro für Infrastrukturmaßnahmen in den Jahren 2021 und 2022 vorgesehen. Aufwendungen für den Personalbereich werden durch das Regelbudget abgedeckt. Der Bedarf an Planstellen wurde ressortintern gedeckt. Darüber hinaus erfordert das Sonderfinanzierungspaket „Cyber-Sicherheit“ der Jahre 2021 und 2022 aus Sicht BMLV ein Folgepaket, um Vorhaben, die in diesen beiden Jahren begonnen werden, fortführen und erweitern zu können.

Zu 6 und 16:

Die Organisationspläne der cyberrelevanten Dienststellen wurden Ende des Jahres 2020 überarbeitet und in Zusammenarbeit mit dem Bundesministerium für Kunst, Kultur, öffentlicher Dienst und Sport erweitert. Daraus ergibt sich eine Steigerung der budgetären Mittel des Personalansatzes im Cyber Bereich des Ressorts. Der Umfang der Aufstellung von zusätzlichen Elementen in den Streitkräften findet derzeit in den Planungen der Projektorganisation „UNSER HEER“ Berücksichtigung.

Zu 11 bis 13:

Im Bereich der nachrichtendienstlichen Cyber-Abwehr liegt der Fokus in der weiteren Aufstellung der Fähigkeit zur Aufklärung von Cyber-Bedrohungen. Im Bereich der CIS-Defence liegt der Fokus in der Erstellung der planerischen Vorgaben für die Umsetzung des Sonderinvestitionspakets im Sinne meiner vorstehenden Ausführungen. Nicht unerwähnt möchte ich lassen, dass darüber hinaus am Aufbau von ersten Rapid Response Teams sowie einem Fachstab Cyber im Rahmen des Kommandos Streitkräfte gearbeitet wird.

Zu 14:

Bis zum Jahr 2024 wird planerisch eine deutliche Steigerung der Fähigkeit im Bereich der Cyber-Sicherheit, insbesondere im Normbetrieb und im Cyberkrisenmanagement erwartet, wenn aufbauend auf das Sonderfinanzierungspaket „Cyber-Sicherheit“ der Jahre 2021 und 2022 ein weiteres Sonderinvestitionspaket beschlossen wird. Die Schaffung von zusätzlichen Fähigkeiten der Cyber-Verteidigung ist konzeptionell bis zum Jahr 2030 mit der Aufstellung von Elementen bei den Streitkräften vorgesehen.

Zu 15:

Die dazu erforderlichen Strukturbearbeitungen finden im Rahmen der Projektorganisation „UNSER HEER“ statt und sind noch nicht abgeschlossen.

Zu 17:

Ja.

Zu 18:

Auf Grund des neuen Organisationsplans können im IKT- & Cybersicherheitszentrum zusätzliche Fachkräfte zu Bedingungen des Bundesdienstes aufgenommen und weitergeschult werden. Das BMLV ist sich jedoch dessen bewusst, dass diese Maßnahme den generellen Druck des Arbeitskräftemangels im IKT-Bereich nicht gänzlich ausgleichen kann. Darüber hinaus ist zu bedenken, dass Bewertungsunterschiede gegenüber anderen Bundesdienststellen und das höhere Lohnniveau in der Privatwirtschaft nur teilweise mit Attraktivierungsmaßnahmen kompensiert werden können. Als längerfristige Maßnahme wurde die Einrichtung des Fachhochschulstudiengangs „Militärinformatik“ an der Theresianischen Militärakademie in die Wege geleitet, um den personellen Aufwuchs von Cyber-Fachpersonal einigermaßen sicher zu stellen.

Zu 19:

Mit dem Sonderfinanzierungspaket „Cyber-Sicherheit“ der Jahre 2021 und 2022 werden, wie in Frage 10 erläutert, finanzielle Schwerpunkte des Aufbaus für die Waffengattungen Cyber- und EloKa-Truppe geschaffen. Dies bedeutet jedoch keine inhaltliche Schlechterstellung der IKT-Truppe, da ein Aspekt der Tätigkeit der Cyber- und EloKa-Truppe auf dem Schutz der Leistungen der IKT-Truppe liegt.

Zu 20:

Das Zusammenwirken der Domänen Land, Luft, Cyber und Information soll in den Streitkräften unter anderem mit dem Aufbau des Fachstabs Cyber geschaffen werden. Die Domäne Information bleibt auf Grund unterschiedlicher Inhalte von der Domäne Cyber getrennt.

Zu 21:

Alle organisatorischen Maßnahmen beziehen sich auf die bestmögliche Erfüllung der gesetzlich festgelegten Aufgaben des Bundesheeres. Da sich Bedrohungen laufend verändern, wird auf Grund entsprechender Analysen im BMLV (Risikobild 2030 und daraus abgeleitete Streitkräftevarianten) eine laufende Anpassung der Organisation vorgenommen werden. Dies betrifft vor allem die umfassende Vernetzung im Cyber-Raum, deren möglichst friktionsfreie Funktionalität für Österreich von höchster Bedeutung ist. Auf Basis eines neuen Streitkräfteprofils wird daher durch die geplanten Organisationsmaßnahmen im Bereich der Cyber-Fähigkeiten sowohl der Selbstschutz des Bundesheeres als auch die

Fähigkeit zur Landesverteidigung im Cyber-Raum sichergestellt und auch die Fähigkeit zur Assistenzleistung bei Cyber-Angriffen auf kritische Infrastrukturen erheblich gestärkt werden.

Mag. Klaudia Tanner

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG @ AMTSSIGNATUR	**Unterzeichner**	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2021-03-19T09:49:11+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur bzw. des Ausdrucks finden Sie unter: http://www.bmlv.gv.at/amtssignatur
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-03-19T09:55:12+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.	