MAG. KLAUDIA TANNER
BUNDESMINISTERIN FÜR LANDESVERTEIDIGUNG

S91143/73-PMVD/2024 5. August 2024

Herrn
Präsidenten des Nationalrates

Parlament
1017 Wien

Die Abgeordneten zum Nationalrat Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 5. Juni 2024 unter der Nr. 18764/J an mich eine schriftliche parlamentarische Anfrage betreffend „Wie steht es um die Cyber Defence?“ gerichtet. Diese Anfrage beantworte ich wie folgt:

Zu 1 bis 1c, 4, 4a, 6 bis 6e und 15:

Maßnahmen, die im Rahmen der Cyber Defence getätigt wurden, sind insbesondere die Implementierung einer bereits arbeitsfähigen Cyber Informations- und Dokumentationszelle in der Abteilung „IKT&Cyber Einsatz“ (IKCyE) und die Miteinbeziehung der zivilen kritischen Infrastruktur im Rahmen der Cyber Defence Übungen „Locked Shields“. Dabei wurde unter anderem gemeinsam mit Institutionen der IT-Infrastruktur sowie des Bank- und Energiewesens die Verteidigung von fiktiver Infrastruktur geübt. Durch die Zusammenarbeit mit Cyberexperten aus der Schweiz im Zuge der „Locked Shields 24“ konnten wichtige Erkenntnisse hinsichtlich des Zusammenwirkens mit zivilen Schlüsselbereichen am Beispiel der Schweiz gewonnen werden, weswegen eine weitere Vertiefung dieser Zusammenarbeit geplant ist. Im Rahmen des Aufbauplans ÖBH2032+ wurden zudem Strukturen und Abläufe eines „Cyber Component Commands“ ausgearbeitet sowie Planungen zur Aufstellung der Cyber-Truppe mit notwendigen Strukturen und Prozessen vorgenommen. Darüber hinaus ist im Aufbauplan ÖBH2032+ eine ständige Führungsbereitschaft auf Basis eines Journaldienstes vorgesehen. Da das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport erst jüngst die Leitungsfunktionen in der Direktion 6 bewertete, war eine permanente Besetzung noch nicht möglich; die Führung der Direktion 6 wurde bis zur Besetzung mit einem mit der Überleitung betrauten Leiter sichergestellt. Zudem wurde zusätzliches Personal dienstzugeteilt.

Zu 1d und 5 bis 5d:

Mögliche Szenarien für das Eintreten eines souveränitätsgefährdenden Cyber-Angriffs sowie dessen völkerrechtliche Beurteilung und Folgeabschätzung sind derzeit in Bearbeitung. Dabei ist auch kritische Infrastruktur als bedeutendes Ziel möglicher souveränitätsgefährdender Cyber-Angriffe berücksichtigt. Anzumerken ist, dass der Schutz der kritischen Infrastruktur und das nationale Krisenmanagement (inklusive Cyber-Krisen) im Zuständigkeitsbereich des Bundesministeriums für Inneres (BMI) liegt. Der Zuständigkeitswechsel zum Bundesministerium für Landesverteidigung (BMLV) erfolgt in Folge der Feststellung eines Verteidigungsfalles durch die Bundesregierung. Das BMLV kann in diesem Fall für Assistenzeinsätze herangezogen werden, sofern die zuständigen Organe des BMI die ihnen zukommende Aufgabe nur unter Mitwirkung des Bundesheeres bewältigen können.

Zu 1e und 3a:

Entfällt.

Zu 2:

Die zentrale Schnittstelle hinsichtlich aller Einsatzangelegenheiten zu anderen Ministerien, insbesondere zum BMI, ist die Abteilung „Militärstrategische Einsatzkoordination“. Die ressortübergreifende bundesweite Koordinierung bzw. Aufgabenteilung wird permanent und auch im Anlassfall mit der gesamtstaatlichen Struktur der Cyber-Sicherheit gemäß der Österreichischen Strategie für Cyber-Sicherheit geregelt.

Zu 3 und 3b:

Das BMLV arbeitet im Rahmen des Cyber Krisenmanagementkonzepts diversen Gremien zu. Im Übrigen verweise ich auf die Zuständigkeit des BMI, das in dieser Angelegenheit federführend ist.

Zu 7:

Es findet ohnehin ein regelmäßiger Informationsaustausch zwischen der Direktion 6 und den beiden militärischen Nachrichtendiensten im Themenbereich statt.

Zu 8, 9, 10a bis 12a und 14:

Der Bereich „Cyber“ umfasst im Aufbauplan ÖBH 2032+ für einen Zeitraum von zehn Jahren 500 Mio. Euro, darunter unter anderem die Budgetmittel zur Aufstellung von etwa 160 Mitarbeitern zur Cyber-Verteidigung, zur Verstärkung des vorhandenen Militär Cyber Zentrums durch die Errichtung einer Cyber Range, die Installation eines Security Operation Centers (SOC) und die Aufstellung von Rapid Response Teams in der Stärke von zumindest

20 Mitarbeitern. Ein zentrales SOC ist im BMLV bereits etabliert und koordiniert regelmäßig Maßnahmen gegen Angriffsversuche bzw. wehrt diese ab; ein SOC mit autarken, verlegbaren Elementen und eine Cyber Range zu Trainingszwecken befinden sich derzeit in Planung. Die Rapid Response Teams sind im Militärischen Cyber Zentrum angesiedelt. Ein Team ist bereits mit entsprechendem Personal und Fähigkeiten ausgestattet und somit verfügbar. Zu den Personalplänen bis 2032 können derzeit noch keine endgültigen Evaluierungen vorgenommen werden, da sie von der Verfügung der Struktur abhängen. Da eine detailliertere Informationen zu diesen Fragen Rückschlüsse auf die Einsatzfähigkeit des ÖBH zuließen, ist eine Beantwortung aus Gründen der Amtsverschwiegenheit im Interesse der umfassenden Landesverteidigung gemäß Art. 20 Abs. 3 B-VG nicht möglich.

Zu 10:

Eine Auswertung der finanziellen Mittel der Budgets der Jahre 2023 und 2024, die ausschließlich den Bereich der Cyber Defence betreffen, ist nicht möglich, da das Bundeshaushaltsgesetz derartige Zuordnungen nicht vorsieht. Es ist jedoch anzumerken, dass die notwendigen Betriebsausgaben für die Cyberabwehr ausreichend bedeckt sind.

Zu 13:

Die Miliz ist ein wichtiger Bestandteil bei Verbindungsdiensten zur nationalen Schlüsselinfrastruktur und der gesamtstaatlichen Zusammenarbeit. Milizarbeitsplätze werden insbesondere zum Abdecken von Spezialkompetenzen sowie zur Sicherstellung der Durchhaltefähigkeit in Stäben und Cyber Einsatzelementen vorgesehen.

Mag. Klaudia Tanner

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG @ AMTSSIGNATUR	**Unterzeichner**	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2024-08-05T07:23:31+02:00
	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.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-05T07:31:02+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	