RN/152

18.48

Präsidentin des Rechnungshofes Dr. Margit Kraker: Sehr geehrter Herr Präsident! Geschätzte Abgeordnete des Hohen Hauses! Heute stehen drei Prüfberichte des Rechnungshofes aus dem Bereich der Landesverteidigung zur Debatte. Die Landesverteidigung besteht ja aus einer primären und originären Kernaufgabe, nämlich der militärischen Landesverteidigung durch das österreichische Bundesheer, und weitere Aufgaben sind subsidiär die Assistenzaufgaben, da geht es um die sicherheitspolizeiliche Assistenz und die Assistenz in Katastrophenfällen.

Die vorliegenden Berichte decken das gesamte Aufgabenspektrum ab, einerseits die militärische Landesverteidigung betreffend die Einsatzfähigkeit der 4. Panzergrenadierbrigade bis hin zu den Leistungen des Bundesheeres im Cyberraum in Form der Cyberdefence sowie die Aufrechterhaltung der militärischen Sicherheit und der Assistenzleistung des Bundesheeres im Blackout-Fall.

Ich komme nun zu den Berichten im Einzelnen. Der erste Bericht, der angesprochen wurde, ist die Cyberdefence. Da geht es um die Koordination der Cyberdefence. Es wurde hier schon besprochen, dass die Cybersicherheit zu den größten globalen Risken zählt und dass durch geopolitische Spannungen und durch neue Tools der künstlichen Intelligenz die Bedrohungslage im Bereich der Cybersicherheit zunimmt. Dementsprechend müssen wir uns dem anpassen und darauf reagieren.

Wir haben uns deshalb bei der militärischen Landesverteidigung das Thema der Cyberdefence angeschaut. Es beschreibt die militärische Landesverteidigung im Cyberraum. Sie umfasst sämtliche vom Bundesheer gesetzte Maßnahmen, um einen Cyberangriff auf die Souveränität Österreichs oder auf Einrichtungen des

Bundesheeres mit militärischen Mitteln abzuwehren. Für den Fall eines Angriffs hat nämlich die Verteidigungsministerin den Eintritt der Souveränitätsgefährdung zu beurteilen. Ihr obliegt es, über den Einsatz zur militärischen Landesverteidigung zu verfügen.

Wir haben uns angeschaut, welche Leistungen das Verteidigungsministerium dabei erbringt und insbesondere auch, wie die Koordination zwischen dem Bundeskanzleramt, dem Innenministerium und anderen Bundesministerien erfolgt. Da gibt es zunächst strategische Grundlagen: die Österreichische Strategie für Cybersicherheit 2021 des Bundeskanzleramts und es gibt das Konzept für ein gesamtstaatliches Cyberkrisenmanagement. Die strategische Grundlage für das Verteidigungsministerium ist dann die Cyberverteidigungsstrategie, die Leitlinie Cyberverteidigung. Diese war im Prüfzeitraum erst im Entwurf vorhanden und wurde dann im Oktober 2023 erlassen.

Im Konzept zum gesamtstaatlichen Cybermanagement waren die konkreten Verantwortlichkeiten bis zur Entscheidung über einen Defence-Einsatz nur in groben Zügen festgelegt. Wir haben daher empfohlen und empfehlen weiterhin, das Konzept mit einer Klarstellung von Verantwortlichkeiten, der Einrichtung von Kommunikationskanälen zwischen den Gebietskörperschaften und innerhalb von Gebietskörperschaften und einer effizienten Koordination zu konkretisieren.

Wir haben auch bemängelt, dass das Verteidigungsministerium noch keine konkreten Kriterien oder Szenarien ausgearbeitet hat, anhand derer beurteilt werden konnte, ob aufgrund eines Cyberangriffes tatsächlich eine Souveränitätsgefährdung vorliegt. Anhand dieser Kriterien könnte eben dann auch entschieden werden, dass ein Cyberdefence-Einsatz getroffen werden muss. Wir meinen, es ist notwendig, in Leitlinien Kriterien und Optionen für die

Feststellung und Bewertung einer Beeinträchtigung der Unabhängigkeit und Funktionsfähigkeit der Einrichtungen von Gebietskörperschaften und die Bedeutung einzelner kritischer Infrastrukturen hinsichtlich der Verletzung der österreichischen Souveränität festzulegen.

Man muss auch darüber nachdenken und klären, welches Ausmaß ein möglicher Angriff erreichen muss, um einen militärischen Einsatz zu rechtfertigen. Das ist notwendig, um im Anlassfall entsprechend reagieren zu können. Es gab ein Cybersicherheitspaket mit 40 Millionen Euro. Da waren einzelne Maßnahmen vorgesehen, aber einige Punkte wie die militärischen Cyberrange-Einsatzteams oder das Security Operations Center wurden nicht umgesetzt; das konnte aufgrund von Personalressourcen nicht umgesetzt werden.

Es gab eine Organisationsreform im Ministerium, um da die Zuständigkeiten zu bündeln. Das haben wir an sich anerkannt. Was wir kritisiert haben: dass spezifische Übungen eines Cyberdefence-Falls aufgrund der Souveränitätsgefährdung nicht durchgeführt wurden. Gesagt wurde uns auch, dass beim gesamtstaatlichen Cyberkrisenmanagement mit der nationalen Umsetzung der NIS2-Richtlinie eine Konkretisierung erfolgen kann. Bei den Übungen wurden teilweise Cyberaspekte mit geübt.

Ich komme nun zur Prüfung der 4. Panzergrenadierbrigade. Da geht es um die Einsatzbereitschaft und um die Möglichkeit zur Aufgabenerfüllung dieser Brigade. Es ist dies eine Prüfung auf Verlangen der FPÖ. Gegenstand der Prüfung waren das Aufgabenspektrum der 4. Panzergrenadierbrigade, die strategischen Konzepte und Planungen, personelle und materielle Ausstattung und die Infrastruktur. Diese Brigade gliedert sich in fünf Verbände mit Standorten in Oberösterreich und Niederösterreich.

Was wir festgehalten haben, ist, dass das Verteidigungsministerium beginnend mit 2011 die Investitionen in die Kampfpanzer reduziert hat. Die Fähigkeiten

sollten nur mehr erhalten werden und rekonstruierbar sein. Ich gebe aber zu bedenken: Wir haben diesen Bericht schon 2023 vorgelegt. Es gab dann im Budgetbegleitgesetz 2023 ein Landesverteidigungs-Finanzierungsgesetz, mit dem man die Mittel für das Verteidigungsressort deutlich aufgestockt hat.

Wir haben außerdem kritisiert, dass trotz dieser eskalierenden Konfliktsituation in der Ukraine seit 2014 nur eine geringe Investitionstätigkeit im Bereich der Kampf- und Schützenpanzer festzustellen war. Wir haben empfohlen, Bereiche dieser Teilstrategie Verteidigungspolitik, die aufgrund der bewaffneten Konflikte nunmehr eine Veränderung der militärischen Fähigkeiten erfordern, neu zu beurteilen. Beim Personalstand haben wir natürlich Mängel gesehen. Der Iststand lag bei Offizieren, Unteroffizieren, Chargen seit 2018 unter 70 Prozent des Sollstandes. Bemängelt wird auch, dass die sicherheitspolizeilichen Assistenzeinsätze die Ressourcen der 4. Panzergrenadierbrigade zusätzlich belasteten.

Wir haben empfohlen, ein digitales Ausbildungscontrolling zu entwickeln, damit die Fähigkeiten auch tatsächlich vermittelt werden konnten. Es gab budgetäre Restriktionen – und das führt zu mangelnden Investitionen. Aufgrund des Alters der Geräte war es oft nicht möglich, Ersatzteile zu beschaffen. Wir haben empfohlen, dass es ein Lebenszyklusmanagement gibt, das eine wichtige Voraussetzung dafür ist, dass man Ersatzinvestitionen zeitgerecht planen kann. Das ist auch wichtig, um rechtzeitig Investitionsentscheidungen zu treffen.

Erheblichen Sanierungsbedarf gab es bei der Infrastruktur, bei den Bauzuständen. Es gab einen hohen Investitions- und Sanierungsbedarf. Wir empfehlen, zeitgerecht die notwendigen Mängel zu beheben.

Die dritte Prüfung wurde auch schon angesprochen. Das sind die geplanten und getroffenen Maßnahmen zur Vorbereitung auf den Blackout-Fall, die wir geprüft haben. Wir haben das als ein sehr relevantes Thema gesehen; denn es ist immer

wichtig, dass man Vorbereitungshandlungen sieht und trifft. Wir haben das als Rechnungshof auf Bundesebene bei Innenministerium und Verteidigungsministerium, auf Landesebene beim Land Steiermark und auf Gemeindeebene bei der Stadtgemeinde Feldbach geprüft.

Wir haben natürlich gesehen, dass das staatliche Krisen- und Katastrophenschutzmanagement des Innenministeriums die zentrale Drehscheibe ist, aber für einen bundesweiten, großflächigen, überregionalen Stromausfall gewisse Zuständigkeiten fehlen; denn die Koordination des SKKM bezieht sich nur auf Aufgaben des Bundes, nicht auch auf die Aufgaben der Länder. Es wäre notwendig, dass für solche Blackout-Fälle, wenn es Österreich wirklich großflächig, gesamt betrifft, ein Kompetenztatbestand geschaffen wird, der die überregionale Koordination vorsieht; und das regen wir im Bericht an.

Wir haben zentrale Elemente herausgearbeitet, was wir für den Blackout-Fall als wirklich notwendig sehen: Es geht um ein gemeinsames Begriffsverständnis von Blackout, es geht um die Definition von Blackout-relevanten Aufgaben und Personal. Das soll natürlich auch zwischen Gebietskörperschaften abgestimmt sein. Es geht um Information und Bewusstseinsbildung und um die Definition jener Bereiche, die mit Notstrom versorgt werden können und die auch immer wieder regelmäßig auf ihre Eignung überprüft werden müssen.

Positiv haben wir die Stadtgemeinde Feldbach hervorgehoben. Die hat umfangreiche, wissenschaftlich begleitete Vorbereitungsmaßnahmen gesetzt. Die Maßnahmen umfassten die Stärkung der Eigenvorsorge der Bevölkerung, die Einrichtung von elf notstromversorgten und fußläufig erreichbaren Selbsthilfebasen, die Sicherstellung der Funktionsfähigkeit der Infrastruktur, der Treibstoffversorgung und die Gewährleistung von Kommunikation und Information. Wir sehen das als ein Best-Practice-Beispiel, das man sicher auch auf andere Gemeinden übertragen könnte.

Das Verteidigungsministerium war bei seinem Projekt der militärischen Autarkie noch nicht so weit. Es geht um 100 Liegenschaften. Das hat man sich bis 2023 vorgenommen. Die Umsetzungsphase war zu kurz und es gab angespannte Personalressourcen. Die vollständige Autarkie war noch in keiner der Liegenschaften erreicht.

Ich bedanke mich für die Aufmerksamkeit. *(Allgemeiner Beifall.)*

18.59

Präsident Peter Haubner: Als Nächster zu Wort gemeldet ist Abgeordneter Harald Thau. – Ich stelle Ihre Redezeit auf 3 Minuten ein, Herr Abgeordneter.