



. PRESSEMITTEILUNG

Abg.z.NR Robert Laimer

SPÖ-Laimer zu Cyberdefence: Österreich muss mehr Ressourcen für das „Schlachtfeld der Zukunft“ bereitstellen

Angekündigten Investition bei Cyberverteidigung fehlt konkrete Zusage – Angriffe auf Institutionen und Wirtschaftsbetriebe müssen strategisch und ressortübergreifend bekämpft werden

Wien / St. Pölten (24. April 2021) – Die unlängst von Verteidigungsministerin Tanner vollmundig angekündigten 100 Millionen Euro zur Bekämpfung von Cyberattacken haben derzeit wenig Substanz. Zudem ist es fraglich, ob die Mittel tatsächlich für die strategische Cyberverteidigung eingesetzt werden. Ein erheblicher Anteil könnte für die elektronische Kampfführung – Störsender, Radaranlagen oder IT-Hardware – aufgewendet werden. Cyberverteidigung bedarf jedoch einer entsprechenden Kommando- und Führungsstruktur für gezielte Operationen. Daher fordert SPÖ-Wehrsprecher Robert Laimer die avisierten Geldmittel in die für operative Cyberdefence erforderlichen personellen Ressourcen zu investieren.

Wie viele Experten ist auch er davon überzeugt, dass – neben der technischen Infrastruktur - auch entsprechend qualitativ hoch ausgebildetes Führungs- und Fachpersonal zur Gefahrenabwehr eingesetzt werden muss, denn Cyber-Angriffe sind „die Bomben“ der modernen Zeit.

Wenn ÖVP-Verteidigungsministerin Tanner vom Workshop „Strategischer Kompass“ der EU-Verteidigungsminister in Lissabon zurückkehrt, wird sie hoffentlich die richtigen Erkenntnisse für die österreichische Landesverteidigung mitgenommen haben. Dazu zählt etwa die Stärkung der Widerstandsfähigkeit gegen alle Formen von Cyberbedrohungen sowie der Schutz vor international agierende Cyberterroristen.

Laut Experten ist eine effektive Gefahrenabwehr von Cyberangriffen in Österreich nur dann umsetzbar, wenn, wie bereits unter Verteidigungsminister a.D. Hans Peter Doskozil vorgesehen, das derzeit in der Streitkräftebasis angesiedelte Informations-Kommunikations-Technologie- und Cybersicherheitszentrum (IKT&CySihZ) direkt dem Generalstab unterstellt wird und die

Kommandostruktur für eine effektive und operative Ausrichtung geändert und angepasst wird. Bislang sind von Ministerin Tanner jedoch keine konkreten Pläne oder Projekte im Kernbereich der Cyberverteidigung mit einem zugehörigen Zeitrahmen benannt worden.

SPÖ-Wehrsprecher Robert Laimer: „Verteidigungsministerin Tanner meinte erst kürzlich, dass wir erkennen müssen, was die neuen Bedrohungsfelder sind. Dieses Faktum ist nicht von der Hand zu weisen. Ergänzend muss jedoch festgehalten werden, dass die Experten im Sicherheitsapparat haargenau wissen, welche Risikobilder in welcher Ausprägung vorhanden sind. Gerade im Rahmen der Cyberdefence hätte Tanner jetzt die Möglichkeit ambitionierte Projekte umzusetzen. Vielleicht sind die für die Cyberverteidigung angekündigten Gelder bis ins Jahr 2024 jedoch nur eine Luftblase, weil dafür noch gar kein Budget erstellt oder beschlossen wurde. Bisher ist es dem Ressort nicht einmal geglückt für alle Teile des IKT- und Cybersicherheitszentrums einen gültigen Organisationsplan mit einem klaren Schwergewicht zur Wahrnehmung der operativen Aufgaben im Cyberdefence-Bereich zu erwirken. Tanner und Co. hinken modernen Strukturen, wie sie in anderen Ländern längst üblich sind, gewaltig hinterher. Da trennen uns Welten.“

Insgesamt sieht Robert Laimer bei der ÖVP-Ministerin weder eine strategisch-operative Ausrichtung der Cyberverteidigung noch eine Konzentration auf die personelle Aufstockung. Diese wäre jedoch, vor dem Hintergrund stark ansteigender Cyberattacken und beträchtlicher Schadenssummen, dringend nötig. Die bisher getätigten Maßnahmen lassen jedoch den Schluss zu, dass den Ankündigungen keine Taten folgen werden.

„Alibi-Handlungen im Rahmen der Umfassenden Landesverteidigung kennen wir von der ÖVP zur Genüge. Dass Verteidigungsministerin Tanner in Lissabon die Zusammenarbeit bei EU-Missionen optimieren möchte, hört sich im ersten Moment gut an. Wenn jedoch zu Hause sämtliche Hausaufgaben – von der Luftraumüberwachung, der Blackout-Prävention bis zum professionellen Ausbau der Cyberverteidigungsstrukturen – unerledigt am Tisch liegen, dann sind die Bekundungen unglaubwürdig. Zuerst gilt es die Souveränität Österreichs zu sichern. Erst danach sollten gutgemeinte Ratschläge bei den EU-Kollegen deponiert werden“, so Laimer abschließend.