

20.48

**Abgeordneter Robert Laimer (SPÖ):** Herr Präsident! Frau Bundesministerin! Meine Damen und Herren! Die russische Invasion in der Ukraine begann im Februar dieses Jahres mit einem Cyberangriff auf Viasat, das ermöglicht die Satellitenkommunikation der Ukraine.

Mittlerweile wird auch öffentlich von digitaler Souveränität gesprochen. Darunter versteht man die Möglichkeit zur selbstbestimmten Nutzung und Gestaltung von Informationstechnik durch Gesellschaft, Staat, Unternehmen und Individuen.

Mit zunehmender Digitalisierung in allen Lebensbereichen haben sich gleichsam auch erhebliche Sicherheitsrisiken aufgetan. Öffentliche Institutionen sowie deren Kommunikations- und Betriebssysteme sind besonders gefährdet, weil sie nicht nur über enorm große sensible Datenmengen verfügen, sondern im Rahmen der Daseinsvorsorge, der Verwaltung der Gesundheit oder der Sicherheit auch relevante Aufgaben für die Allgemeinheit übernehmen. Es ist daher kein Wunder, dass Kriminelle, aber auch staatsnahe Akteure permanent auf der Suche nach Schwachstellen sind, um gezielte Angriffe zu starten.

Wie verwundbar unser Staat ist, haben wir bei dem Hackerangriff auf das Außenministerium im Jahr 2020 gesehen. Es hat mehrere Wochen bis zu dessen Abwehr gedauert. Was lässt sich daraus ableiten? – Sicherheit muss umfassend, gesamtstaatlich und vor allem auch operationalisiert werden. Dazu braucht es professionelle Strukturen und hoch qualifizierte Spezialisten.

Aus diesem Grund unterstützen wir auch den Antrag der NEOS aus dem Jahr 2020 zum Aufbau eines Stabes Cyberdefence und werden in der Folge dazu einen eigenständigen Entschließungsantrag einbringen. Dabei ist anzumerken, dass die Regierungsparteien geschlagene zwei Jahre benötigten, um sich überhaupt einmal damit zu beschäftigen.

Wir bringen daher folgenden Entschließungsantrag ein:

## Entschließungsantrag

der Abgeordneten Robert Laimer, Kolleginnen und Kollegen betreffend „Sicherheit umfassend denken, für echten Schutz unserer Infrastruktur“

Der Nationalrat wollte beschließen:

„Die Bundesministerin für Landesverteidigung wird aufgefordert, bei der Planung der Budgetmittel ab 2023 darauf Bedacht zu nehmen, dass für den Schutz der kritischen Infrastruktur vor Sabotage, insbesondere bei der Wasserversorgung, der Verkehrsinfrastruktur, der Telekommunikation oder der Energieversorgung, ausreichend Budgetmittel zur Verfügung gehalten werden. Über die Verwendung der Budgetmittel zum Schutz der kritischen Infrastruktur vor Sabotage soll dem Nationalrat und dem Bundesrat ein Bericht vorgelegt werden, der zeigt wie diese Mittel konkret eingesetzt wurden.“

\*\*\*\*\*

Abschließend auch von meiner Person ein Dank an unseren Kollegen Reinhard Bösch. Wir bleiben in der Parlamentarischen Bundesheerkommission weiterhin kollegial verbunden. – Vielen Dank. *(Beifall bei der SPÖ sowie bei Abgeordneten von ÖVP, FPÖ, Grünen und NEOS.)*

20.51

*Der Antrag hat folgenden Gesamtwortlaut:*

## Entschließungsantrag

*der Abgeordneten Robert Laimer, Genossinnen und Genossen*

*betreffend Sicherheit umfassend denken, für echten Schutz unserer Infrastruktur*

*eingebraucht im Zuge der Debatte über den Bericht des*

*Landesverteidigungsausschusses über den Antrag 686/A(E) der Abgeordneten*

*Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend Aufbau eines Stabes Cyberdefense (1741 d.B.)*

*Die Welt ist unsicherer geworden: Kriege, Umweltkatastrophen, Angriffe im digitalen Raum und die Instabilität der Energiemärkte sind nur vier Bereiche, die unsere Sicherheitsinfrastruktur auf die Probe stellen können und die Sicherheit gefährden. Drohende Black-outs, beispielsweise auf Grund von fehlenden Energielieferungen oder Schwankungen im Netz, die latente Bedrohung, irgendwann doch und trotz der guten geopolitischen Lage Österreichs Ziel eines feindlichen Sabotageaktes zu werden, oder aber auch die sich zuspitzenden Wetterphänomene, die zu Überschwemmungen, Vermurungen und Bränden führen, haben zugenommen und führen uns vor Augen – es gibt viel zu tun, um die Sicherheit der Bevölkerung zu gewährleisten.*

*All diese Szenarien bedeuten für die Sicherheit in Österreich massive Bedrohungslagen, denen es durch entsprechende Vorbereitungen rechtzeitig entgegenzuwirken gilt, bevor sie eintreten. Eine Schlüsselrolle muss dabei das Österreichische Bundesheer spielen.*

*Dazu braucht es einerseits die Stärkung der Dienste Heeresnachrichtenamt und Heeresabwehramt, die vor allem im Bereich der Beobachtung von kriegerischen Auseinandersetzungen, terroristischer Bedrohungen im digitalen aber auch im analogen Bereich sowie im Bereich der geopolitischen Lage zentrale Aufgaben erfüllen. Zugleich ist aber auch ein Fokus auf den Schutz kritischer Infrastruktur, wie der Versorgung mit Wasser, Strom, Energie, der Verkehrsinfrastruktur oder aber auch dem Internet, zu legen. Dieses ist mittlerweile zentraler Teil der Infrastruktur und somit auch der Daseinsvorsorge geworden. Gerade deshalb ist die Schaffung zusätzlicher Strukturen, die sich insbesondere mit Cybercrime, vor allem aber auch mit Cyberdefense auseinandersetzen, unabdingbar.*

*Waren es, wie die Zeitschrift „Strategische Horizonte“ in ihrer ersten Ausgabe im Jahr 2022 beschreibt im Ersten Weltkrieg die Eisenbahnen, die eine massive Veränderung des Kriegsgeschehens nach sich gezogen hat, so sind es heute digitale*

Mittel, die maßgeblich dafür sind, Staaten zu destabilisieren oder gar die öffentliche Ordnung und Sicherheit zum Erliegen zu bringen. Dabei geht es einerseits natürlich um Cyberangriffe, wie beispielsweise auf das Land Kärnten im Sommer 2022 oder zuvor auf das Außenministerium im Februar 2022. Es geht zugleich aber auch um die Sicherheit von Steuerungen in Kraftwerken, dem Bereich der öffentlichen Verwaltung oder der Gesundheitsversorgung, die hier dringend vor Bedrohungen aus dem digitalen Raum geschützt werden müssen. Digitale Bedrohungen sind also mittlerweile genauso bedrohlich für die Infrastruktur und somit die Menschen in Österreich geworden, wie Umweltkatastrophen oder die Unsicherheit im Zusammenhang mit der Energieversorgung.

Die grundsätzlich begrüßenswerte und längst überfällige Erhöhung des Verteidigungsbudgets ist dafür der Schlüssel – für eine umfassende Sicherheits- und Verteidigungspolitik braucht es die entsprechenden Mittel. Diese Erhöhung muss aber strategisch sinnvoll genutzt und entsprechend weitblickend eingesetzt werden, was bedeutet, dass definiert sein muss, wofür man das zusätzliche Budget einsetzt.

Wichtig ist, dass dabei auf die Bedrohungslagen, die existieren, Bedacht genommen wird. So zeigte sich mit dem Verdacht eines Sabotageaktes rund um die Hauptkolonne der OMV, dass Infrastruktur, die für die tägliche Versorgung der Menschen relevant ist, auf jeden Fall ausgeschlossen oder das Risiko zumindest minimiert werden muss. Auch die Beschädigungen auf den Bahnstrecken der Deutschen Bahn in Norddeutschland, bei der Glasfaserkabelstränge durchtrennt wurden, zeigen, dass mit Bedacht und Insiderwissen auch politisch motivierte und durch andere Staaten gesetzte Sabotageakte nicht mehr undenkbar sind und einer entsprechenden Vorbereitung bedürfen, um nach Möglichkeit verhindert werden zu können.

Während schon bei der Präsentation des Heeresbudgets eine eindeutige Botschaft zeigte wohin die Reise bei der Verteilung der zusätzlichen Mitteln zu gehen scheint – die Verteidigungsministerin trat dabei im Beisein von Bundeskanzler Nehammer und Finanzminister Brunner vor Radpanzern und schwerbewaffneten, maskierten Soldaten auf – braucht es im Sinne der Bevölkerung ein Bekenntnis dazu, dass diese

Mittel im Sinne des Schutzes der kritischen Infrastruktur und der Daseinsvorsorge eingesetzt werden.

Aus diesem Grund stellen die unterfertigten Abgeordneten folgenden

### *Entschließungsantrag*

Der Nationalrat wolle beschließen:

„Die Bundesministerin für Landesverteidigung wird aufgefordert, bei der Planung der Budgetmittel ab 2023 darauf Bedacht zu nehmen, dass für den Schutz der kritischen Infrastruktur vor Sabotage, insbesondere bei der Wasserversorgung, der Verkehrsinfrastruktur, der Telekommunikation oder der Energieversorgung, ausreichend Budgetmittel zur Verfügung gehalten werden. Über die Verwendung der Budgetmittel zum Schutz der kritischen Infrastruktur vor Sabotage soll dem Nationalrat und dem Bundesrat ein Bericht vorgelegt werden, der zeigt wie diese Mittel konkret eingesetzt wurden.“

\*\*\*\*\*

**Präsident Ing. Norbert Hofer:** Der Entschließungsantrag ist ordnungsgemäß eingebracht, er steht somit auch mit in Verhandlung.

Zu Wort gelangt nun Mag.<sup>a</sup> Romana Deckenbacher. – Bitte, Frau Abgeordnete.