

---

**686/A(E) XXVII. GP**

---

Eingebracht am 17.06.2020

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

## ENTSCHLIESSUNGSANTRAG

**der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen  
betreffend Aufbau eines Stabes Cyberdefense**

Der Cyberangriff auf das BMEIA Anfang dieses Jahres offenbart die Verwundbarkeit essentieller österreichischer Regierungseinrichtungen gegenüber gezielten Attacken aus dem Ausland. Die *Sicherheitspolitische Jahresvorschau 2020* merkt an, dass integrierte Technologien, die Schwachstellen gegen Cyberrangriffe darstellen, vermehrt in kritischer Infrastruktur, wie Spitälern, der Verwaltung auf allen Ebenen, Kraftwerken und der Industrie Anwendung finden, und Österreich gegenüber staatlichen und kriminellen Akteuren vulnerabel machen.

In Anfragebeantwortung 1465 A/B vom 8 Juni 2020 schreibt Bundesministerin Klau-  
dia Tanner, eine "in Einheiten und Verbänden selbstständig strukturierte „**Cybermi-  
liz**“ **ist nicht geplant**, Cybermilizkomponenten bzw. Milizarbeitsplätze sind aber in  
verschiedenen Organisationsbereichen vorgesehen."

Im "Starlinger Papier" *Unser Heer 2030* wird Cybersecurity als die Basis zur Sicher-  
stellung der Führungsfähigkeit in Friedens- und Einsatzzeiten bezeichnet, deren Aus-  
fall "die Einsatzbereitschaft und Wirkungsfähigkeit des ÖBH massiv einschränkt" und  
"somit die Gefahr für Kollateralschäden erhöht." Auch das interne Strategiepapier  
*Vision Landesverteidigung 2020* bezieht sich auf den Cyberangriff auf das BMEIA.  
Das Starlinger Papier verlangt den "Aufbau einer Cybertruppe und eines Trainings-  
zentrums für den Kampf im Cyberspace."

Ministerin Tanner verweist in Anfragebeantwortung 679A/B zu einer Anfrage zum  
Thema BMEIA Cyberangriff auf das Regierungsprogramm 2020 bis 2024 und spezi-  
fisch auf das Kapitel "Landesverteidigung und Krisen- und Katastrophenschutz" und  
hebt: "im konkreten Zusammenhang ... Themen, wie etwa Weiterentwicklung der  
Kernkompetenzen sowie aller Teilstreitkräfte Land, Luft, Spezialeinsatzkräfte und  
**Cyberkräfte**, Anpassung des Österreichischen Bundesheeres an aktuelle Bedro-  
hungslagen, wie **Cyber Defense** und hybride Bedrohungen, Prioritärer Ausbau der  
**Cyber-** und **Drohnenabwehrfähigkeiten** und **Ausbau einer Cyber-Truppe unter  
besonderer Berücksichtigung der Ausbildungserfordernisse für Cyber-  
Defense-Personal und Mitwirkung am nationalen Cyberlagezentrum und am  
gesamtstaatlichen Cybersicherheitszentrum**, besonders" hervor.

Im Landesverteidigungsausschuss vom 03.03.2020 erklärte die Bundesministerin,  
der jüngste Cyberangriff auf das Außenministerium zeige die Notwendigkeit des  
Ausbaus der Cyber-Abwehr auf. Es gelte, zusätzliches Know-how zu gewinnen und

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

die Abwehrfähigkeit im Cyberbereich weiter zu entwickeln. Konkret wollte Tanner das Cyberfrühwarnsystem verstärken und eine **Cybertruppe mit eigenen Ausbildungserfordernissen aufbauen** (Parlamentskorrespondenz Nr. 190 vom 3.3.2020).

In Anbetracht der sich ständig von konventioneller auf Cyberspace verschiebenden Bedrohungslage ist es wichtig, für die Sicherheit der kritischen Infrastruktur und der Einsatzbereitschaft des Bundesheeres klare Cyberdefense Strukturen zu schaffen.

Die unterfertigten Abgeordneten stellen daher folgenden

## ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

"Die Bundesministerin für Landesverteidigung wird aufgefordert, dem Nationalrat ehestmöglich, aber nicht später als Ende 2020, eine Regierungsvorlage zuzuleiten, die die Erschaffung einer eigenständigen Cyberdefense Einheit im Landesverteidigungsministerium vorsieht. Dabei soll der Risikoeinschätzung in der Sicherheitspolitischen Jahresvorschau 2020 und anderen strategischen Analysen des BMLV besonders Rechnung getragen werden."

*In formeller Hinsicht wird die Zuweisung an den Landesverteidigungsausschuss vorgeschlagen.*