12060/J XXVII. GP

Eingelangt am 31.08.2022

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Dr. Helmut Brandstätter, Kolleginnen und Kollegen

an die Bundesministerin für Landesverteidigung

betreffend Status des Cybersicherheitsstabs und der HNA Befugnisse

In der Ausgabe vom 27.08.2022 berichtet *Der Spiegel* in seiner Titelstory über russische Geheimdiensttätigkeiten in Europa, von der Unterwanderung von Sanktionen (seit dem ersten Sanktionspaket 2014) über Spionage, politische Manipulationen bis hin zu Attentaten und Morden. Der Bericht kommt zum Schluss, dass Deutschland seit dem Ende des Kalten Krieges erstens seine Nachrichtendienste nicht ausreichend ausgestattet hat, und zweitens kein wirkliches Interesse daran hatte, das Putin Regime zu verärgern. So wurden die Bewegungen von regimenahen Prominenten (wie zum Beispiel einer von Vladimir Putins Töchtern) nicht nachverfolgt, und mit Spionage im Zusammenhang stehende Diplomat_innen nicht ausgewiesen. Das Resultat: Deutschland muss heute fürchten, dass wichtige Teile der kritischen Infrastruktur kompromittiert und Institutionen unterwandert sind.

Auch Österreich hat in den letzten Jahren ein ähnliches Nahverhältnis zum Putin Regime aufgebaut. Die Abhängigkeiten vom russischen Energiemarkt sind vergleichbar. Auch hat Österreich ein im internationalen Vergleich extrem schwaches Spionagegesetz, in dem Spionageaktivitäten nicht einmal strafbar sind, wenn sie sich nicht gegen Interessen der Republik richten.

Die Probleme mit der Spionageabwehr sind in Österreich gut bekannt. Bereits 2020 merkt die *Sicherheitspolitische Jahresvorschau* 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. Damit wird Österreich gegenüber staatlichen und kriminellen Akteuren vulnerabel. Im Starlinger Papier *Unser Heer 2030* wird der "Aufbau einer Cybertruppe und eines Trainingszentrums für den Kampf im Cyberspace" explizit verlangt. Und Ministerin Tanner hebt in Anfragebeantwortung 679/AB "Themen, wie etwa Weiterentwicklung der ... Cyberkräfte, Anpassung des Österreichischen Bundesheeres an aktuelle Bedrohungslagen, wie Cyberdefense und hybride Bedrohungen, prioritärer Ausbau der Cyber- und Drohnenabwehrfähigkeiten und Ausbau einer Cyber-Truppe unter besonderer Berücksichtigung der Ausbildungserfordernisse für Cyberdefense-Personal und Mitwirkung am nationalen Cyberlagezentrum und am gesamtstaatlichen Cybersicherheitszentrum" besonders hervor.

Dennoch wurde im Außenpolitischen Ausschuss am 17. Juni 2020 ein Antrag von den Regierungsparteien vertagt, der diesem Problem durch die Schaffung eines Cyberstabes im BMLV entgegenwirken wollte. Die Regierungsparteien begründeten die *de-facto* Ablehnung mit den bereits fortgeschrittenen Aktivitäten der Bundesministerin.

Am 9. Juni 2022 wurde ein Antrag von den Regierungspartien vertagt, der notwendige Anpassungen der Befugnisse der Nachrichtendienste an die technologischen Veränderungen des 21. Jahrhunderts sowie Anpassung der Befugnisse an die Standards der europäischen Partnerdienste vorschlug. Das Argument der Regierungsparteien war auch hier, dass dieser Antrag berechtigt, aber bereits in Arbeit sei.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wo steht das BMLV in Hinblick auf den von der Ministerin beschriebenen prioritären Ausbau der Cyber- und Drohnenabwehrfähigkeiten?
    a. Welche spezifischen Fortschritte wurden seit Vertagung des Antrags gesetzt?
2. Wo konkret steht die von der Ministerin versprochene "Cyber-Truppe unter besonderer Berücksichtigung der Ausbildungserfordernisse für Cyberdefense-Personal"?
    a. Welche nächsten konkreten Schritte sind geplant?
3. Wie genau wirkt das BMLV am nationalen Cyberlagezentrum und am gesamtstaatlichen Cybersicherheitszentrum mit?
4. Bis wann werden die in den Antworten zu Fragen 1-3 gesetzten Schritte abgeschlossen sein?
5. Wo steht die Reform von §20 des Militärbefugnisgesetzes? Welche Fortschritte wurden seit Vertagung des Antrags zu diesem Thema gemacht?
    a. Hat das BMLV einen Vorschlag für eine Novellierung erarbeitet?
        i. Wenn ja, wann wird dieser dem Nationalrat vorgelegt?
        ii. Wenn nein, wann ist mit einer derartigen, von den Diensten dringend geforderten Novellierung zu rechnen?
6. Welche anderen Schritte hat das BMLV gesetzt, um sich spezifisch im gegenwärtigen Krieg gegen Cyberattacken zu wappnen?
    a. Mit welchen anderen Ministerien arbeitet das BMLV in Hinblick darauf zusammen und wie sieht diese Zusammenarbeit aus?