10206/J XXVII. GP

Eingelangt am 18.03.2022

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesministerin für Landesverteidigung

betreffend Cyberbedrohungen infolge des Krieges in der Ukraine

Bereits in der Vorbereitungsphase auf den russischen Überfall auf die Ukraine wurden Vermutungen geäußert, dass ein russischer Angriff mit Cyberattacken gegen strategische Ziele, wie kritische Infrastruktur, Regierungs- und Kommandostrukturen eingeläutet werden würde. Tatsächlich gab es vor dem Angriff Cyberattacken gegen die Ukraine, wenn auch in geringerem Ausmaß als angenommen.

Seit Kriegsbeginn haben sich Europa und die USA auf scharfe Sanktionen gegen Russland geeinigt. Internationale Unternehmen tragen diese Sanktionen oft auch schon vor Inkrafttreten mit, oder übererfüllen sie, zum Beispiel mit Rückzügen aus Russland, Aussetzen von Exporten nach oder Vertrieb in Russland. Damit setzen sich diese unternehmen und Regierungen möglichen Vergeltungsmaßnahmen vonseiten Russlands aus, das in den letzten Jahren eine intensive Cyberkapazität aufgebaut hat. Bekannt wurden insbesondere Eingriffe in Wahlen in den USA, aber auch Versuche der Beeinflussung in Europa.

Neben Vergeltungsangriffen sind auch reine Störaktionen möglich, um die Kosten des Sanktionsregimes für die westliche Koalition zu erhöhen und öffentliche Meinung gegen die harten Sanktionen einzunehmen. Auch hat Russland seit langem versucht, seine Position im Westen mittels Propagandamedien zu verbreiten. Sputnik und Russland Heute wurden als Reaktion von der Europäischen Kommission die Lizenzen entzogen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Cyberdefense ist in Österreich Querschnittsmaterie. Wie teilen sich BMLV, BMI und BMEIA die Überwachung und Bedrohung von Cybergefahren auf?

2. Ist seit Beginn des russischen Militäraufmarsches zu Beginn 2021 ein Anstieg der Cyberangriffe oder der Bedrohungen in Österreich oder gegen österreichische Interessen im Ausland festzustellen?
    a. Wenn ja, bitte um eine Größenordnung des Anstiegs.
    b. Welche Ziele werden vorrangig angegriffen, Regierung, Unternehmen, andere?
3. Ist seit Ausbruch des Krieges am 24. Februar ein Anstieg der Cyberangriffe oder der Bedrohungen in Österreich oder gegen österreichische Interessen im Ausland festzustellen?
    a. Wenn ja, bitte um eine Größenordnung des Anstiegs.
4. Wie bewertet das HNA die Cyberaktivitäten Russlands seit Beginn des russischen Aufwuchses vor einem Jahr bzw. seit Kriegsausbruch im Ausland?
    a. Gibt es eine Analyse zu Cyberattacken gegen die Ukraine?
    b. Es wurden überraschend wenige Cyberattacken gegen die Ukraine vor Kriegsausbruch bekannt. Ist dieser Umstand einer funktionierenden Cyberdefense geschuldet? Wenn ja, gibt es Lektionen für Österreich?
5. Wie ist die Lage bei der Nutzung von Fake Accounts in den Sozialen Medien zum Zwecke der Beeinflussung der öffentlichen Meinung zu bewerten? Gibt es eine vom BMLV beobachtete Kampagne in diese Richtung?
    a. Welche Abwehrmaßnahmen werden gegen derartige Kampagnen gesetzt bzw. geplant?