2038/J
vom 18.10.2018 (XXVI.GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesminister für Landesverteidigung

betreffend Maßnahmen des Verteidigungsministers im Bereich Cyberdefense

Nach Angaben der niederländischen und der britischen Regierung steckt der russische Militärgeheimdienst GRU hinter einer Reihe von Cyber-Angriffen auf westliche Staaten und internationale Institutionen wie die Organisation für das Verbot chemischer Waffen (OPCW). Darunter sind auch Institutionen, die etwa mit der Aufklärung des Absturzes der Malaysia Airlines Maschine MH17 im Jahr 2014 über einem von russischen Rebellen dominierten Teil der Ukraine befasst sind sowie mit der Aufklärung des Giftanschlages auf Sergej und Yulia Skripal im März 2018. Die veröffentlichten Erkenntnisse des britischen nationalen Cybersicherheitszentrums (NCSC) und der niederländischen Behörden zeigt deutlich, dass Russland gezielt politische und andere Prozesse manipuliert und unterminiert, die essenziell für das Funktionieren der europäischen Gesellschaft sind.

Gleichzeitig floriert die Online-Kriminalität wie nie zuvor, Angreifer professionalisieren sich. "Innerhalb kurzer Zeit können schlecht gesicherte Infrastrukturen attackiert und fremdgesteuert werden. Aus diesem Grund müssen Unternehmen und öffentliche Institutionen dafür sorgen, ihre Sicherheitslücken zu schließen", hieß es bei einer Pressekonferenz des Bundesheeres Anfang Oktober 2018 anlässlich der IKT-Sicherheitskonferenz in Alpbach. Oberst Walter Unger, Leiter des Cyber-Verteidigungszentrums, betonte in diesem Zusammenhang die dringende Notwendigkeit vermehrter internationaler Zusammenarbeit, um sich vor diesen Gefahren zu schützen und sich gegen Attacken von außen zu verteidigen (derstandard.at/2000088988787/Bundesheer-Cyberbedrohung-immer-groessere-Herausforderung-fuer-Oesterreich).

Im Rahmen der Budgetverhandlungen 2018 wurden Sie als Bundesminister gefragt, wie Österreichs Teilnahme an den PESCO-Projekten im Verteidigungsbereich, darunter auch ein Cybersecurity-Projekt (Cyber Threats and Incident Response Information Sharing Platform), budgetiert sei. Damals hieß es, es gäbe noch kein Budget dafür, weil der Entwicklungsstand der Projekte noch nicht so weit fortgeschritten sei, dass man sich über den anfallenden finanziellen Aufwand im Klaren sei. Mittlerweile ist einige Zeit vergangen und die Dringlichkeit, die europäische Zusammenarbeit in diesem Bereich auf ordentliche Beine zu stellen ist angesichts der zuvor beschriebenen Verhältnisse eindeutig gewachsen.

Die unterfertigenden Abgeordneten stellen daher folgende

Anfrage:

1. Gibt es mittlerweile im BMLV eine Vorstellung davon, wieviel Geld Österreich für seine Teilnahme an den vier PESCO-Projekten aufwenden wird?
   a) Wenn ja, bitte um Aufstellung nach Projekt und Verwendungszweck.
   b) Wenn nein, warum nicht?
2. Bitte um genaue Beschreibung der Zielsetzung des PESCO-Cyberprojekts, an dem Österreich mitwirkt, samt Zeitplan. Was bedeutet "Plattform zum Informationsaustausch" im Zusammenhang des Projekts?
   a) Geht es dabei um ein elektronisches Übermittlungssystem oder um regelmäßiges Zusammentreffen?
   b) Welche Art von Information soll ausgetauscht werden und inwiefern wäre das Projekt eine Verbesserung zum Status quo?
3. Welche Aufgaben übernimmt Österreich konkret bei diesem PESCO-Projekt?
   a) Wie viele Angehörige des Österreichischen Bundesheeres, bzw. wie viele Personen aus dem Verwaltungsbereich sind für die Umsetzung des PESCO-Cyberprojekts eingesetzt? Bitte um Aufschlüsselung nach Aufgabengebiet.
4. Sind auch andere Ministerien in die Durchführung dieses Projektes eingebunden?
   a) Wenn ja, welche?
   b) Wenn ja, wie viele Angehörige anderer Ministerien arbeiten an dem Projekt mit? Bitte um Aufschlüsselung nach Aufgabengebiet.
5. Wie ist das PESCO-Projekt in Österreichs gesamte Cyberstrategie eingebettet?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-10-18T15:52:13+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	