Deutscher Bundestag **Drucksache 19/17282**

19. Wahlperiode 19.02.2020

Kleine Anfrage

der Abgeordneten Andrej Hunko, Heike Hänsel, Gökay Akbulut, Ulla Jelpke, Niema Movassat, Dr. Alexander S. Neu, Thomas Nord, Tobias Pflüger und der Fraktion DIE LINKE.

Militärmanöver „Multi-Lateral Cyber Defence Exercise 20“ in Deutschland

Die Bundeswehr plant im August 2020 ein gemeinsames Manöver zur Cyberkriegführung (Antwort auf die Schriftliche Frage 69 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/16423). Die Übung mit dem Titel „Multi-Lateral Cyber Defence Exercise 20“ (MLCD20) soll im August in Deutschland stattfinden; neben dem israelischen Militär nehmen Einheiten aus Österreich und der Schweiz daran teil. Welche Abteilungen die ausländischen Streitkräfte entsenden, wollte der Parlamentarische Staatssekretär Dr. Peter Tauber trotz Nachfrage nicht mitteilen. In Israel wird die geheimdienstliche Aufklärung im Cyberspace von der militärischen „Einheit 8200“ durchgeführt („Army beefs up cyber-defense unit as it gives up idea of unified cyber command“, www.timesofisrael.com vom 14. Mai 2017). Israelischen Medienberichten zufolge ist die Einheit mittlerweile auch für Cyberangriffe zuständig. Aus der Bundesrepublik Deutschland sind alle wichtigen militärischen Cyberabteilungen an der MLCD20 beteiligt, die Führung liegt bei dem vor drei Jahren aufgestellten Kommando Cyber- und Informationsraum (KdoCIR) in Bonn. Es ist unter anderem für die Aufklärung von Aktivitäten zuständig. Für eigene Cyberangriffe („Planen, Vorbereiten, Führen und Durchführen von Operationen zur Aufklärung und Wirkung“, vgl. http://g1eft.de/3rO) verfügt das Kommando über ein Zentrum Cyber-Operationen (KCO) in Rheinbach. Schließlich nimmt auch das militärische Forschungsinstitut Cyber Defence und Smart Data (CODE) an MLCD20 teil. Zu den dort angenommenen Szenarien ist bislang nichts bekannt. Bei derartigen Übungen werden vom Zentrum Cyber-Operationen (ZCO) der Bundeswehr Angriffe von sogenannten „Red Teams“ simuliert und von „Blue Teams“ gekontert (vgl. Bundestagsdrucksache 19/11920, Antwort zu Frage 19).

Wir fragen die Bundesregierung:

1. Welche gemeinsamen Übungen oder Ausbildungsmaßnahmen (auch im Rahmen der NATO) hat die Bundeswehr mit der israelischen, österreichischen oder schweizerischen Armee seit der Antwort der Bundesregierung auf Bundestagsdrucksache 19/6574 durchgeführt (bitte soweit möglich mit Datum, Teilnehmenden und Ort angeben)?
2. Wann, und wo soll die „Multi-Lateral Cyber Defence Exercise 20“ (MLCD20) im August 2020 in Deutschland stattfinden?

3. Welche Abteilungen bzw. Einheiten des Militärs (auch Militärgeheimdienste) aus Israel, Österreich und der Schweiz sind nach Kenntnis der Bundesregierung an der Übung MLCD20 beteiligt?
   a) Welche dieser Einheiten können und dürfen nach Kenntnis der Bundesregierung im Rahmen der Gesetze ihrer Entsendestaaten Cyberangriffe nicht nur abwehren, sondern auch durchführen?
   b) Falls auch das Zentrum Cyber-Operationen (KCO) in Rheinbach teilnimmt, mit welchen Aufgaben?
   c) Welche Aufgaben übernimmt das militärische Forschungsinstitut Cyber Defence und Smart Data (CODE)?
   d) Werden auch Beobachter eingeladen oder erwartet?
4. Welche Abteilungen bzw. Einheiten welcher Militärs bereiten nach Kenntnis der Bundesregierung die Übung MLCD20 vor, welche Treffen zur Vorbereitung der Übung MLCD20 haben bereits stattgefunden, und wer nahm daran teil?
5. Welche Rahmenlage wird nach gegenwärtigem Stand für die Übung MLCD20 angenommen?
6. Welche Szenarien oder Vorkommnisse werden nach gegenwärtigem Stand in MLCD20 geübt (sofern diese noch nicht feststehen, bitte die Schwerpunkte skizzieren)?
   a) Werden nach gegenwärtigem Stand auch Desinformationen und Kampagnendynamik in sozialen Medien simuliert?
   b) Sollen nach gegenwärtigem Stand auch „offensive Cyberoperationen“ durchgeführt bzw. trainiert werden?
   c) Werden in der Übung MLCD20 auch Cyberangriffe simuliert, die einen bewaffneten Angriff im Sinne von Artikel 51 der VN-Charta darstellen?
   d) Wird auch Sabotage, Diebstahl und Manipulation sensibler Daten (etwa bei Unternehmen) simuliert (vgl. „Tausende Firmen, öffentliche Einrichtungen und Behörden gefährdet“, www.swr.de vom 13. Januar 2020)?
7. An welchen Cyberübungen der Europäischen Union oder der NATO hat sich die Bundeswehr mit welchen Abteilungen seit der Antwort der Bundesregierung auf Bundestagsdrucksache 19/11920 mit „Red-Teams“ beteiligt?
8. Kommen bei der Übung MLCD20 sogenannte „Red Teams“ zum Einsatz, und was wird dazu erwogen, welche Abteilungen bzw. Einheiten welcher Militärs diese übernehmen sollen?
9. Welche Vereinbarungen kennt die Bundesregierung zwischen der Computer Incident Response Capability (NCIRC) der NATO und dem EU-Computer Emergency Response Team (CERT-EU), und wie werden diese umgesetzt?
10. Inwiefern haben die Bundeswehr oder Geheimdienste der Bundesregierung bereits „Software-Artefakte“ in kritischen Infrastrukturen anderer Staaten eingesetzt, und auf welchen völkerrechtlichen Rechtsgrundlagen erfolgte dies (Bundestagsdrucksache 19/11920, Antwort zu Frage 9)?
11. Welche Details kann die Bundesregierung zum regelmäßigen bilateralen „Austausch zu Cyberthemen im Finanzsektor“ mit Israel mitteilen (Bundestagsdrucksache 19/11920, Antwort zu Frage 8)?

12. Wie unterstützt die Bundesregierung die Umsetzung der von Russland eingebrachten UN-Resolution „Countering the use of information and communications technologies for criminal purposes“ (https://digitallibrary.un.org/record/3831879)?

13. Unter welchen Voraussetzungen hält es die Bundesregierung für angemessen, als Reaktionen auf einen Cyberangriff auf das Schengener Informationssystem SIS II sämtliche EU-Außengrenzen für die Dauer des Ausfalls zu schließen, wie es im Rahmen der EU-Krisenmanagementübung EU HEX -ML 18 (PACE) geübt worden ist (Bundestagsdrucksache 19/16241, Antwort zu Frage 22)?

14. Was ist der Bundesregierung hinsichtlich der „Cyber-Konsultationen“ zwischen der Europäischen Union und der NATO darüber bekannt, inwiefern dort auch gemeinsame Krisenreaktionsmechanismen behandelt werden?

15. Auf welche Weise beteiligt sich die Bundesregierung an der Aufklärung der Cyberangriffe auf Behörden in Österreich („Attacke auf Österreichs Außenministerium – Bundesheer hilft bei Abwehr“, www.tagesspiegel.de vom 15. Januar 2020), welche Erkenntnisse hat sie zu den mutmaßlichen Urhebern, und worauf stützt sie diese?

16. Auf welche Weise sind Bundesbehörden mit Ermittlungen zu dem mutmaßlichen Cyberangriff auf das Berliner Kammergericht befasst („Datenproblem an Berliner Kammergericht schwerer als erwartet“, www.tagesspiegel.de vom 27. Januar 2020), und kann die Bundesregierung bestätigen, dass dort Daten abgeflossen sind?

17. Was kann die Bundesregierung zum aktuellen Stand ihrer Überlegungen für eine „aktive Cyber-Abwehr“ mitteilen, bzw. wann sollen die Prüfungen hierzu abgeschlossen sein (vgl. Bundestagsdrucksache 19/11920)?

    a) Inwiefern erwägt die Bundesregierung sogenannte „Hackbacks“ auch bei Angriffen, die von Systemen traditioneller Geheimdienste ausgehen?

    b) Inwiefern erwägt die Bundesregierung „Hackbacks“ auch bei Angriffen, die von Systemen befreundeter Geheimdienste ausgehen?

Berlin, den 28. Januar 2020

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333