Deutscher Bundestag **Drucksache 19/18497**

19. Wahlperiode 02.04.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/17282 –

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

Vorbemerkung der Fragesteller

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://gleft.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).

Vorbemerkung der Bundesregierung

Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann [BVerfGE 124, 161 (189)]. Die Bundesregierung ist nach sorgfältiger Abwägung zu der

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 1. April 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Auffassung gelangt, dass die Angaben zu Ausbildungsmaßnahmen mit den Streitkräften Österreichs, Israels und der Schweiz (Frage 1), die Nennung der Einheiten dieser Nationen an der Übung „Multi-Lateral Cyber Defence Exercise 20“ (Frage 3) sowie die Teilnahme von „Red Teams“ der Bundeswehr an Cyberübungen der Europäischen Union und der NATO (Frage 7) aus Geheimhaltungsgründen nicht in dem für die Öffentlichkeit einsehbaren Teil bereitgestellt werden.

Der parlamentarische Informationsanspruch ist grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Im vorliegenden Fall ist im Hinblick auf das Staatswohl die Einstufung dieser Informationen als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ erforderlich.*

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)?

Die Bundeswehr hat seit Beantwortung der Bundestagsdrucksache 19/6574 folgende gemeinsame Übungen mit den israelischen, österreichischen oder schweizerischen Streitkräften durchgeführt:

Datum	Übung	Teilnehmende Organisationen	Ort
12.02.2019	Tri-nationale Luftwaffenübung	Österreichisches Bundesheer Schweizer Armee	Deutschland Österreich Schweiz
14.03.2019 – 01.04.2019	SURVEYING TEAMS 2019	Österreichisches Bundesheer	Deutschland
28.03.2019 – 17.04.2019	ALLIED SPIRIT 2019	Israelische Streitkräfte	Deutschland
07.04.2019 – 12.04.2019	ELEPHANT RECOVERY	Österreichisches Bundesheer Schweizer Armee	Deutschland
12.05.2019 – 17.05.2019	Live Firing exercise	Israelische Streitkräfte	Griechenland
17.05.2019 – 18.05.2019	Notfall- und Brandschutzübung 2019	Österreichisches Bundesheer	Österreich
03.06.2019 – 14.06.2019	CAPABLE LOGISTICIAN	Österreichisches Bundesheer	Polen
17.06.2019 – 21.06.2019	Network Operational Führung Exercise	Schweizer Armee	Deutschland
03.07.2019	Tri-nationale Luftwaffenübung	Österreichisches Bundesheer Schweizer Armee	Deutschland Österreich Schweiz

* Das Bundesministerium der Verteidigung hat Teile der Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Datum	Übung	Teilnehmende Organisationen	Ort
04.08.2019 – 20.09.2019	MIGHTY WAVES	Israelische Streitkräfte	Israel
16.08.2019 – 27.08.2019	EUROPEAN GUARDIAN	Österreichisches Bundesheer	Österreich
16.09.2019 – 11.10.2019	Informations- und Lehrübung Landoperationen	Österreichisches Bundesheer	Deutschland
14.10.2019 – 31.10.2019	EUROPEAN FALCON	Österreichisches Bundesheer	Deutschland
03.11.2019 – 15.11.2019	BLUE FLAG 2019	Israelische Streitkräfte	Israel
18.11.2019 – 29.11.2019	EUROPEAN ADVANCE 2019	Österreichisches Bundesheer	Österreich
09.03.2020 – 27.03.2020	Übung „EUROPEAN CHALLENGE 2020“	Österreichisches Bundesheer	Deutschland

Hinsichtlich Ausbildung mit den Streitkräften Österreichs, Israels und der Schweiz unterhält die Bundeswehr eine ausgeprägte Kooperation mit allen drei Ländern. Eine Aufstellung der Maßnahmen der Bundeswehr mit diesen Nationen seit Beantwortung der Bundestagsdrucksache 19/6574 enthält die „VS – Nur für den Dienstgebrauch“ eingestufte Anlage.

2. Wann und wo soll die „Multi-Lateral Cyber Defence Exercise 20“ (MLCD20) im August 2020 in Deutschland stattfinden?

Die Übung MULTI-LATERAL CYBER DEFENCE EXERCISE 20 (MLCD20) wird vom 3. bis 7. August 2020 an der Universität der Bundeswehr in München durchgeführt.

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?

Auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage wird verwiesen.

a) Welche dieser Einheiten können und dürfen nach Kenntnis der Bundesregierung im Rahmen der Gesetze ihrer Entsendestaaten Cyberangriffe nicht nur abwehren, sondern auch durchführen?

Der Bundesregierung liegen keine Erkenntnisse vor, welche dieser Einheiten im Rahmen der Gesetze ihrer Entsendestaaten Cyberangriffe nicht nur abwehren, sondern auch durchführen können und dürfen.

b) Falls auch das Zentrum Cyber-Operationen (KCO) in Rheinbach teilnimmt, mit welchen Aufgaben?

Das Zentrum Cyber-Operationen nimmt an der Übung MLCD20 nicht teil.

c) Welche Aufgaben übernimmt das militärische Forschungsinstitut Cyber Defence und Smart Data (CODE)?

Das Forschungsinstitut Cyber Defence und Smart Data (CODE) stellt für die Durchführung von MLCD20 die dortige CyberRange Umgebung und Personal zur technisch-administrativen Betreuung der Teilnehmer zur Verfügung.

d) Werden auch Beobachter eingeladen oder erwartet?

Es werden Beobachter eingeladen und 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?

Von deutscher Seite bereitet das Kommando Cyber- und Informationsraum der Bundeswehr die Übung MLCD20 vor. Es liegen keine Erkenntnisse darüber vor, welche Abteilungen bzw. Einheiten in Israel und Österreich die Übung vorbereiten. Bisher haben keine Treffen zur Vorbereitung der Übung MLCD20 mit externen Teilnehmern außerhalb des Kommandos Cyber- und Informationsraum der Bundeswehr stattgefunden.

5. Welche Rahmenlage wird nach gegenwärtigem Stand für die Übung MLCD20 angenommen?

Nach gegenwärtigem Stand ist noch keine Rahmenlage 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)?

Es stehen noch keine Szenarien oder Vorkommnisse fest. Der Schwerpunkt der Übung MLCD20 liegt auf Security Operations Center (SOC)-Training im Rahmen der Behandlung von Cyber Incidents.

a) Werden nach gegenwärtigem Stand auch Desinformationen und Kampagnendynamik in sozialen Medien simuliert?

Nein.

b) Sollen nach gegenwärtigem Stand auch „offensive Cyberoperationen“ durchgeführt bzw. trainiert werden?

Nein.

c) Werden in der Übung MLCD20 auch Cyberangriffe simuliert, die einen bewaffneten Angriff im Sinne von Artikel 51 der VN-Charta darstellen?

Nein.

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)?

Nein.

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?

Auf die als „VS – Nur für den Dienstgebrauch“ wird verwiesen.

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?

Bei der Übung MLCD20 kommen nach gegenwärtigem Stand keine „Red Teams“ zum Einsatz.

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?

Die NATO Computer Incident Response Capability (NCIRC) und das EU-Computer Emergency Response Team (CERT-EU) haben am 10. Februar 2018 eine Technische Vereinbarung zum Austausch von nicht als Verschlusssache eingestuften Informationen geschlossen. NATO und EU berichteten im Fortschrittsbericht „Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017” vom 17. Juni 2019 über die Zusammenarbeit von NCIRC und CERT-EU. Danach arbeiten die beiden Institutionen zusammen, tauschen Informationen über die Malware Information Sharing Platform (MISP) aus und führen regelmäßige Gespräche zum Austausch über technische Aspekte durch.

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)?

Im Sinne der Anfrage erfolgte kein Einsatz von „Software-Artefakten“ in kritischer Infrastruktur anderer Staaten.

11. Welche Details kann die Bundesregierung zum regelmäßigen bilateralen „Austausch zu Cyberthemen im Finanzsektor“ mit Israel mitteilen (Bundestagsdrucksache 19/11920, Antwort zu Frage 8)?

Das Bundesministerium der Finanzen hat sich insbesondere in zwei Gesprächsrunden mit Israel zu Cyberthemen im Finanzsektor ausgetauscht. Im Rahmen der 8. Sitzung des FintechRats am 8. Juni 2019 wurde der Israelische National Fintech-Cyber Innovation Lab vom israelischen Finanzministerium vorgestellt.

Im Rahmen des ersten deutsch-israelischen Finanzdialogs im November 2019 wurde der Austausch fortgesetzt.

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)?

Die Bundesregierung hat – wie alle Mitgliedstaaten der Europäischen Union – die am 27. Dezember 2019 mehrheitlich angenommene Resolution der VN-Generalversammlung „Countering the use of information and communication technologies for criminal purposes“, die die Erarbeitung eines neuen VN-Instruments vorsieht, nicht unterstützt. Die Bundesregierung sieht zwar den Bedarf an weiteren Maßnahmen zur effektiven Bekämpfung von Straftaten auf diesem Gebiet, sie erkennt aber keine Notwendigkeit für einen neuen völkerrechtlichen Vertrag im Rahmen der Vereinten Nationen. Die Bundesregierung befürchtet, dass ein solcher den Schutz der Menschenrechte und der Grundfreiheiten absenken und staatliche Kontrolle über das Internet fördern könnte. Die Bundesregierung betrachtet die auch für Nicht-Mitgliedstaaten des Europarates offene Budapest Convention weiterhin als das prioritäre Mittel zur Bekämpfung von Straftaten auf diesem Gebiet, auch mit Blick auf den dort verbürgten Rechtsschutzstandard. Die weiteren Prozesse, die auf die mehrheitlich angenommene VN-Resolution folgen, werden von der Bundesregierung verfolgt und gegebenenfalls mitgestaltet.

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)?

Die Durchführung von Grenzkontrollen an den Schengen-Außengrenzen richtet sich nach der Verordnung (EU) 2016/399 (Schengener Grenzkodex). Im Übrigen äußert sich die Bundesregierung zu hypothetischen Fragestellungen nicht.

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?

Der Austausch von NATO und EU im Cyber-Bereich beinhaltet unter anderem auch den Austausch zu Aspekten der Krisenreaktionsmechanismen. Im Juni 2018 sowie im April 2019 wurden Workshops veranstaltet, um die Mitarbeiter mit den Prozeduren und Mechanismen der jeweils anderen Organisation vertraut zu machen. Auf die Antwort zu Frage 9 wird verwiesen.

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?

Im Rahmen der internationalen Zusammenarbeit unterstützen deutsche Bundesbehörden auf der Grundlage ihrer Zuständigkeiten und Befugnisse ausländische Partner. Aufgrund laufender Ermittlungen in Österreich können derzeit keine Auskünfte erteilt werden, ohne den Untersuchungszweck zu gefährden.

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?

Das Bundeskriminalamt unterstützt die Berliner Behörden bei den polizeilichen Ermittlungen. Dem Bundeskriminalamt liegen derzeit keine validen Informationen darüber vor, ob und in welchem Umfang in diesem Zusammenhang Daten abgeflossen sind. Im Übrigen nimmt die Bundesregierung zu laufenden Ermittlungsverfahren grundsätzlich keine Stellung, um den Fortgang der Ermittlungen nicht zu gefährden.

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)?

Die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen werden derzeit von der Bundesregierung umfassend geprüft. Diese Prüfungen sind noch nicht abgeschlossen.

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?

Die Fragen 17, 17a und 17b werden wegen des Sachzusammenhangs zusammen beantwortet.

Der von den Fragestellern verwendete Begriff „Hackback“ wird von der Bundesregierung konzeptionell nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage legt die Bundesregierung die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung in der Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 19/2645 zugrunde. Die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen werden derzeit von der Bundesregierung umfassend geprüft. Auf die Antwort der Bundesregierung zu Frage 9 auf Bundestagsdrucksache 19/2645 wird verwiesen. Diese Prüfungen sind noch nicht abgeschlossen.

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