Deutscher Bundestag **Drucksache 19/1212**

19. Wahlperiode 14.03.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/929 –

Beteiligung an Cyberübungen der EU und der NATO im Jahr 2018

Vorbemerkung der Fragesteller

Unter der estnischen Ratspräsidentschaft hat die Europäische Union im vergangenen Jahr Cyberübungen zur gemeinsamen Krisenbewältigung durchgeführt (Bundestagsdrucksache 18/13503). Den Anfang macht die eintägige Stabsübung „EU CYBRID 2017“, in deren Simulation ein EU-Hauptquartier „multiplen Cyberattacken“ ausgesetzt war. Wenige Wochen später folgt die Übung „EU PACE 17“, bei der „eine erhebliche Anzahl von EU-Mitgliedstaaten“ von Cyberangriffen „unterschiedlicher Natur und Intensität“ betroffen gewesen sein soll. Die Szenarien in „EU CYBRID 2017“ und „EU PACE 17“ sollten „die grenzüberschreitende und ressortübergreifende Zusammenarbeit im Krisenmanagement in einem hybriden Umfeld“ üben. Während der simulierten Störungen waren die Teilnehmenden unter anderem von einem „erhöhtem und gesteuertem Falschmeldungsaufkommen“ betroffen. In einer späteren Phase nahmen die Ministerien und Behörden an der parallel verlaufenden NATO-Übung „CMX 17“ teil. Auch die dortigen Übungsszenarien umfassten „Fake News“. Zu den Teilnehmenden gehörte das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), das sich wie die EU-Übungsleitung ebenfalls in Tallinn befindet. Aus Deutschland waren das Bundesministerium der Verteidigung und die Bundeswehr beteiligt.

Während der Übungen wurden täglich neue Ereignisse („Injektionen“) simuliert. Die britische Bürgerrechtsorganisation Statewatch hatte hierzu ein Planungspapier veröffentlicht (http://gleft.de/26o). Demnach wurden in „EU PACE 17“ gleich mehrere Bedrohungen für die Europäische Union angenommen. Ein „quasi-demokratisches Land“ stellte sich dabei mit seiner wirtschaftlichen und militärischen Macht gegen die Europäische Union. Aus Sicht der Fragestellerinnen und Fragesteller war hiermit Russland angedeutet, das in der Übung als „Froterre“ bezeichnet wurde. Die Regierung des Fantasiestaates verfügte außerdem über „Hacker, Hacktivisten und nationale Medien“, die ebenfalls gegen die Europäische Union zu Felde zogen. Wesentliche Akteure waren die Hackergruppen „APT Fabelwolf“ und „APT Schimärenwolf“, die vermutlich auf die beiden Russland zugeschriebenen Gruppen APT 28 und APT 29 anspielen. Als zweite große Bedrohung wurde in „EU PACE 17“ ein „Neugeborener Extremistenstaat“ (NEXSTA) simuliert, der ein weltweites Kalifat erschaffen wolle. Durch Überredung, Druck und Terror wollen die Kalifatskrieger

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 12. März 2018 übermittelt.

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

ihre Kultur in Europa verbreiten. Zwar nutzt NEXSTA Mittel der digitalen Propaganda, verfügt aber nur über geringe Cyberfähigkeiten. Zum weiteren Gegenspieler der Europäischen Union machte „EU PACE 17“ Geflüchtete im Mittelmeer. Ihre Fluchthelfer wurden im angenommenen Szenario vom Militär in einer „Operation AIFOS“ bekämpft: aus Sicht der Fragestellerinnen und Fragesteller eine deutliche Anspielung auf die real existierende EU-Militärmission EUNAVFOR MED Sophia. Außerdem simulierten die EU-Cyberkrieger auch die Bekämpfung einer „Antiglobalisierungsgruppe“. Sie wurde in dem Szenario als internationale Bewegung beschrieben, deren besondere Fähigkeit im „Organisieren von Krawallen, die sich als Demonstrationen tarnen“, liegt. Geld für ihre Aktionen erhält die „Antiglobalisierungsgruppe“ vom Fantasiestaat „Froterre“.

Schließlich hat sich die Bundeswehr im vergangenen Jahr auch an der „NATO-Cyber-Abwehr-Übung Locked Shields 2017“ beteiligt (Bundestagsdrucksache 18/13503). Als Szenarien galten „Verunstaltung von Webseiten, Verbreitung von Falschmeldungen, Datendiebstahl von Benutzernamen und Passwörtern, Übernahme der Steuerung von militärischen Drohnen, Ausschalten der Energieversorgung eines Militärflughafens, Kontrolle über die Flugzeugbetankungsanlage“.

Vorbemerkung der Bundesregierung

Die von den Fragestellerinnen und Fragestellern genannten Übungen decken ganz unterschiedliche Übungsspektren ab, welche von strategischen Übungen mit Anteilen aus dem Cyberraum (z. B. „Crisis Management Exercise“ – CMX – bzw. „Parallel and Coordinated Exercise“ – PACE) bis hin zu Übungen zu technischen Einzelaspekten (z. B. „Locked Shields“) reichen. Für strategische Übungen spielen Szenarien eine große Rolle, während diese bei technischen Übungen eher vernachlässigbar sind. Gleichzeitig bilden Übungsinhalte, welche den Cyberraum betreffen, in strategischen Übungen nur einen geringen Anteil ab, wogegen in technisch fokussierten Übungen nahezu ausschließlich diese Facette betrachtet wird.

Vor dem Hintergrund der notwendigen Unterscheidung und des Fokus der Fragesteller auf „Cyberübungen“ werden die Antworten zu den Fragen 1, 3 und 9 auf die Aspekte des Cyberraumes fokussiert.

Eine andere Rolle nimmt die – ebenfalls von den Fragestellerinnen und Fragestellern genannte – „EU CYBRID 2017“ ein. Wenngleich als Übung zu nennen, ist „EU CYBRID 2017“ eher mit einem Workshop zur Sensibilisierung für die Herausforderungen politischer Erstbewertung und Entscheidungsfindung im Umgang mit Cyber-Zwischenfällen zu vergleichen.

1. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „PACE 18“ bekannt?

   a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

Die Übung soll vom 12. bis 30. November 2018 in Brüssel (Belgien), Larissa (Griechenland), Nea Santa (Griechenland), Torrejon (Spanien) und den jeweiligen teilnehmenden Staaten durchgeführt werden.

b) Welche Szenarien werden dort geübt?

Es werden sowohl zivile als auch militärische Krisenreaktionsszenarien im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) geübt. Die Übung wird nach derzeitigem Stand sowohl aus Planungsaufgaben als auch aus eventbasierten Aufgaben, d. h. eingespielten Ereignissen bestehen. Das geopolitische Umfeld setzt sich aus den Regionen Europa und Afrika sowie dem damit verbundenen maritimen Bereich zusammen.

c) Wer ist mit der Planung und Koordinierung beauftragt?

Die Übung wird im engen Zusammenwirken zwischen dem Europäischen Auswärtigen Dienst (EAD) und der Europäischen Kommission geplant und koordiniert.

d) Wer soll an der Übung teilnehmen, bzw. wer wird hierzu (auch als Beobachter) eingeladen?

Dazu liegen der Bundesregierung noch keine Informationen vor.

e) Welche Vorübungen sollen hierzu abgehalten werden?

Zu Vorübungen liegen der Bundesregierung keine Erkenntnisse vor.

f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

Auf die Antwort zu Frage 1e wird verwiesen.

g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „PACE 18“ beteiligen?

Dazu liegt aktuell noch keine Entscheidung vor.

2. Wann und wo wurde bzw. wird die Krisenmanagementübung „PACE 17“ ausgewertet?

3. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „PACE 17“?

Die Fragen 2 und 3 werden aufgrund ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Eine Auswertung wurde durch das Planning Team des EAD durchgeführt. Innerhalb der Bundesregierung ist der Auswerteprozess derzeit noch nicht abgeschlossen.

4. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „EU CYBRID 2018“ bzw. eine ähnliche, aber anderslautende Veranstaltung bekannt?

a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

b) Welche Szenarien werden dort geübt?

c) Wer ist mit der Planung und Koordinierung beauftragt?

d) Wer soll an der Übung teilnehmen, bzw. wer wird hierzu (auch als Beobachter) eingeladen?

e) Welche Vorübungen sollen hierzu abgehalten werden?

f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „EU CYBRID 2017“ beteiligen?

Die Fragen 4 bis 4g werden aufgrund ihres inhaltlichen Zusammenhanges gemeinsam beantwortet.

Eine Übung „EU CYBRID 2018“ ist der Bundesregierung nicht bekannt.

5. Wann und wo wurde bzw. wird die Krisenmanagementübung „EU CYBRID 2017“ ausgewertet?

Eine Auswertung erfolgte durch die damalige estnische EU-Ratspräsidentschaft im Anschluss an das informelle Treffen der EU-Verteidigungsminister am 6. und 7. September 2017.

6. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „EU CYBRID 2017“?

Die Übung diente der Sensibilisierung der Teilnehmer für die Herausforderungen der politischen Erstbewertung und Entscheidungsfindung in einem hybriden Cyberszenario sowie der Einübung der Anwendung bestehender EU-Krisenreaktions-mechanismen. Da die Reaktion auf eine Krise in einem hybriden oder Cyber-Kontext der politischen Steuerung bedarf, müssen entsprechende Bedrohungslagen von Anfang an auch auf politischer und strategischer Ebene wahrgenommen und koordiniert werden. Die Bundesregierung begrüßt die Initiative der damaligen estnischen EU-Ratspräsidentschaft. Ein gemeinsames Verständnis von hybriden und Cyber-Bedrohungen ist notwendig. Aus Sicht der Bundesregierung belegte „EU CYBRID 2017“ insbesondere die Bedeutung der notwendigen Kooperation zwischen EU und NATO in diesem Bereich.

7. Was ist der Bundesregierung über die Planungen für eine Krisenmanagement-übung „CMX 18“ bzw. eine ähnliche, aber anderslautende Veranstaltung der NATO bekannt?

a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

b) Welche Szenarien werden dort geübt?

c) Wer ist mit der Planung und Koordinierung beauftragt?

d) Wer soll an der Übung teilnehmen, bzw. wer wird hierzu (auch als Beobachter) eingeladen?

e) Welche Vorübungen sollen hierzu abgehalten werden?

f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

Die Fragen 7 bis 7f werden aufgrund ihres inhaltlichen Zusammenhanges gemeinsam beantwortet.

Nach Kenntnissen der Bundesregierung ist keine Krisenmanagementübung der NATO „CMX 18“ geplant.

g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „CMX 17“ beteiligen?

Bei der Übung „CMX 17“ haben die deutsche NATO-Vertretung, das Bundesministerium der Verteidigung, das Auswärtige Amt und das Bundesministerium des Innern teilgenommen. Mit Blick auf die Frage nach einer Krisenmanagementübung der NATO „CMX 18“ wird auf die Antwort zu den Fragen 7 bis 7f verwiesen.

8. Wann und wo wurde bzw. wird die Krisenmanagementübung „CMX 17“ ausgewertet?

9. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „CMX 17“?

Die Fragen 8 und 9 werden aufgrund ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Die Auswertung und Analyse der Erkenntnisse aus der „CMX 17“ dauert in den zuständigen NATO-Gremien noch an.

10. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „Locked Shields 2018“ bzw. eine ähnliche, aber anderslautende Veranstaltung der NATO bekannt?

„Locked Shields“ ist eine Übungsserie von jährlichen technischen Cyber-Abwehrübungen, die durch das NATO akkreditierte Cooperative Cyber Defence Centre of Excellence (CCD COE) geplant und durchgeführt werden. Formell ist „Locked Shields“ damit keine NATO-Übung. Die Übungsserie dient der Ausbildung des Personals zum Schutz von Computernetzwerken.

a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

Die Übung „Locked Shields 2018“ findet im Zeitraum 23. bis 27. April 2018 in Tallinn beim CCD COE statt. Das Personal zum Schutz von Computernetzwerken (sog. Blue-Teams) nimmt online aus seinen jeweiligen Standorten teil.

b) Welche Szenarien werden dort geübt?

Die Szenarien für „Locked Shields 2018“ sind der Bundesregierung noch nicht bekannt.

c) Wer ist mit der Planung und Koordinierung beauftragt?

Die Planung und Koordinierung ist Aufgabe des CCD COE.

d) Wer soll an der Übung teilnehmen, bzw. wer wird hierzu (auch als Beobachter) eingeladen?

Zur Teilnahme an der Übung sind eingeladen:

- Mitgliedstaaten des CCD COE;
- Nationen, mit denen Beitrittsverhandlungen zum CCD COE vor dem Abschluss stehen;
- das NATO-akkreditierte Computer Incident Response Capability (NCIRC) Element und das EU-Computer Emergency Response Team (EU-CERT).

e) Welche Vorübungen sollen hierzu abgehalten werden?

Nach Kenntnis der Bundesregierung sind keine Vorübungen geplant.

f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

Es wird auf die Antwort zu Frage 10e verwiesen.

g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „Locked Shields 2018“ beteiligen?

An „Locked Shields 2018“ beteiligt sich die Bundesregierung mit einem Blue-Team, im Kern gestellt durch das Zentrum für Cyber Sicherheit der Bundeswehr und Einzelpersonalgestellungen von Fachpersonal aus anderen Dienststellen (auch ressortübergreifend).

11. Wann und wo wurde bzw. wird die Krisenmanagementübung „Locked Shields 2017“ ausgewertet?

Die Übung wurde durch CCD COE und die beteiligten Nationen ausgewertet.

12. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der „Locked Shields 2017“?

Die Übung erfüllt nach Auffassung der Bundesregierung das Ziel der Beübung von Verfahren und Prozessen zum Schutz von Computernetzwerken und dient auch dem Gewinn und dem Transfer fachlicher Expertise.

13. Für wie realistisch hält die Bundesregierung die in der „NATO-Cyber-Abwehr-Übung Locked Shields 2017“ angenommenen Szenarien „Verunstaltung von Webseiten“, „Datendiebstahl von Benutzernamen und Passwörtern“, „Übernahme der Steuerung von militärischen Drohnen“, „Ausschalten der Energieversorgung eines Militärflughafens“, „Kontrolle über die Flugzeugbetankungsanlage“?

Aus Sicht der Bundesregierung sind die angenommenen Szenarien sehr unterschiedlich und auch unterschiedlich realistisch, aber technisch plausibel.

a) Bei welchen Gelegenheiten war die Bundesregierung mit entsprechenden Vorfällen bereits konfrontiert?

Bezüglich der in der Fragestellung genannten Szenarien sind der Bundesregierung Einzelfälle im Bereich Datendiebstahl und Veränderung von Netzseiten bekannt.

Wegen der noch laufenden Analysen und Sicherungsmaßnahmen bleibt der IVBB-Vorfall (IVBB – Informationsverbund Berlin–Bonn) bei dieser Antwort unberücksichtigt.

b) Bei welchen dieser Vorfälle waren die Systeme der Behörden bereits zuvor von „verschiedene[n] Angriffe[n], wie z. B. Phishing-Mails, Innentätern oder Ausnutzung technischer Schwachstellen“ betroffen?

Es wird auf die Antwort zu Frage 13a wird verwiesen.

14. Welche Aufgaben werden das NATO CCDCoE, die „EU Hybrid Fusion Cell” sowie das Kommunikationszentrum „EU STRATCOM EAST“ im Rahmen möglicher Übungen „PACE 18“, „EU CYBRID 2018“, „CMX 18“ (oder anderslautender Veranstaltungen der NATO) und „Locked Shields 2018“ übernehmen?

Bezüglich „PACE 2018“ wird auf die Antwort zu Frage 1 verwiesen. Bezüglich „EU CYBRID 2018“ wird auf die Antwort zu Frage 4 verwiesen. Bezüglich „CMX 18“ wird auf die Antwort zu Frage 7 verwiesen. Bezüglich „Locked Shields 2018“ wird auf die Antwort zu Frage 10c verwiesen. Darüber hinaus sind der Bundesregierung keine Informationen über die Aufgaben oder Beteiligungen der genannten Bereiche an den beschriebenen Übungen in 2018 bekannt.

15. An welchen weiteren Cyberübungen wird sich die Bundeswehr im Jahr 2018 beteiligen, und welche Szenarien werden dort geübt?

Die Bundeswehr plant die Beteiligung an den Übungen „Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise“ (CWIX), „Cyber Coalition 2018“ und „Locked Shields 2018“. Zum Szenario von „Locked Shields 2018“ wird auf die Antwort zu Frage 10b verwiesen. Die Szenare der anderen Übungen sind ebenfalls noch nicht bekannt.

16. An welchen der Cyberübungen, an denen sich die Bundeswehr im Jahr 2018 beteiligt, nimmt auch das „Kommando Computer-Netzwerk-Operationen“ (CNO) teil?

Das Zentrum Cyberoperationen wird an den Übungen „CWIX 2018“, „Cyber Coalition 2018“ und „Locked Shields 2018“ teilnehmen.

17. Inwiefern hält es die Bundesregierung derzeit für notwendig oder entbehrlich, Cyberübungen auch oberhalb der Schwelle eines bewaffneten Angriffs durchzuführen (bitte begründen)?

Um dem im Weißbuch 2016 formulierten Auftrag, Deutschlands Souveränität und territoriale Integrität zu verteidigen und seine Bürgerinnen und Bürger zu schützen, gerecht zu werden, sind Übungen zielführend und notwendig. Das Aufgabenspektrum reicht dabei von der Landes- und Bündnisverteidigung bis zum Zivil- und Katastrophenschutz und umfasst das gesamte Intensitätsspektrum.

Dies gilt auch für den Cyber- und Informationsraum. Auch die „Cyber-Sicherheitsstrategie für Deutschland“ vom 9. November 2016 begründet den Übungsbedarf für den Cyber- und Informationsraum. Hier steht insbesondere der Abstimmungs- und Koordinierungsbedarf der beteiligten Akteure innerhalb der Bundesregierung im Vordergrund.

18. Welche der Cyberübungen, an denen sich die Bundeswehr im Jahr 2018 beteiligt, operieren an der Schwelle eines bewaffneten Angriffs?

Die Szenare der in der Antwort zu Frage 15 aufgeführten Übungen sind der Bundesregierung noch nicht bekannt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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