Deutscher Bundestag **Drucksache 18/13503**

18. Wahlperiode 05.09.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/13271 –

Cyberübungen der EU und der NATO und ihr mögliches Überschreiten der Schwelle eines bewaffneten Angriffs

Vorbemerkung der Fragesteller

Am 7. September 2017 will der informelle EU-Verteidigungsministerrat in Tallinn (Estland) die Cyberübung „EU CYBRID 2017“ abhalten (http://gleft.de/1NL). Damit will die Europäische Union die gemeinsame strategische Krisenreaktion auf einen großen Cyberangriff proben (http://gleft.de/1NM). Die Übung steht unter der Verantwortung des Europäischen Auswärtigen Dienstes und soll das Bewusstsein für „Cybereffekte“ auf politischer und ministerieller Ebene schärfen. Zu probende Szenarien sind bislang nicht bekannt. Die Fragesteller gehen aber davon aus, dass es um die Kooperation der zuständigen operationellen Hauptquartiere in den EU-Mitgliedstaaten geht. Ebenfalls unklar ist, ob sich die Cyberübung auch oberhalb der Schwelle eines bewaffneten Angriffs bewegt. Dies würde bedeuten, dass der Cyberraum zum Austragungsort eines Konfliktes wird, der durch einen konventionellen Angriff auf einen Mitgliedstaat begann.

Für die Vorbereitung der Cyberübung hat die estnische Regierung jetzt eine Ausschreibung veröffentlicht (http://gleft.de/1NN). „EU CYBRID 2017“ findet unter estnischer Präsidentschaft statt. Womöglich aus diesem Grund wird die Übung möglicherweise gemeinsam mit dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) organisiert, das sich ebenfalls in Tallinn befindet. Erste Gespräche des estnischen Verteidigungsministeriums mit der NATO hierzu haben bereits stattgefunden. Ebenfalls im September 2017 will die Europäische Union die fünfwöchige „Krisenmanagementübung 2017 – EU PACE17“ starten (http://gleft.de/1Og). Sie verfolgt sie ähnliche Ziele und Szenarien wie „EU CYBRID 2017“ und findet in einem Setting regelmäßiger Cyberangriffe sowie zunehmender „Fake News“ mit fünf „Bedrohungen“ statt. Hierzu gehören die Bekämpfung von „Migrantenschmuggel“; die Politik gegenüber einem Staat der wirtschaftlich und militärisch mächtiger wird, aber der westlichen Welt zuwiderlaufende Interessen vertritt und hierzu gut ausgebildete Hacker sowie staatliche Medien in Stellung bringt; eine terroristische religiöse Sekte, die ein weltweites Kalifat errichten will; eine globalisierungskritische Gruppe die gut in Sozialen Medien vertreten ist und militante Proteste organisiert und hierzu

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 4. September 2017 übermittelt.

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

finanzielle Mittel von Ländern erhält, die der Europäischen Union feindlich gegenüberstehen; sowie zwei Akteure im Cyberraum mit dem Kürzel „APT“, die militärische Einrichtungen und Ölkonzerne als Hacker angreifen und dabei mit dem Staat in Verbindung stehen, der der westlichen Welt zuwiderlaufende Interessen vertritt.

Mit „Locked Shields“ hält die NATO selbst Cyberübungen ab. Zuletzt wurde die jährliche Übung vom 24. bis zum 28. April 2017 in Tallinn durchgeführt (http://gleft.de/1NP). Beteiligt waren mehrere europäische Verteidigungsministerien sowie das Europa-Kommando der USA. In Schlussfolgerungen fordert der Rat der EU eine engere Zusammenarbeit der NATO und der Europäischen Union gegen Cyberangriffe und „hybride Bedrohungen“ (http://gleft.de/1NO). Zu den Kooperationen gehören außerdem Trainingskurse und Cyberübungen. Zu den Abwehr „hybrider Bedrohungen“ haben die Europäische Union und die NATO außerdem ein „Zentrum gegen hybride Bedrohungen“ („Hybrid-Kompetenzzentrum“) in Helsinki eingerichtet.

1. Was ist der Bundesregierung über die Teilnehmenden und Durchführenden der Cyberübung „EU CYBRID 2017“ sowie etwaiger Vorübungen bekannt, und wann genau finden diese statt?

Die Übung EU CYBRID 17 findet am 7. September 2017 im Rahmen eines informellen Verteidigungsministertreffens statt und wird von der estnischen Ratspräsidentschaft durchgeführt. Teilnehmen werden die Verteidigungsminister der EU-Mitgliedstaaten plus max. drei Stabsmitglieder, das estnische Verteidigungsministerium, die Europäische Verteidigungsagentur, die European Network Information Security Agency, das EU Intelligence Analysis Centre und Vertreter der Integrated Political Crisis Response Kontaktstellen sowie der Europäische Auswärtige Dienst (EAD). Zu Vorübungen liegen der Bundesregierung keine Informationen vor.

2. Was ist der Bundesregierung über die Teilnehmenden und Durchführenden der Krisenmanagementübung „EU PACE17“ sowie etwaiger Vorübungen bekannt, und wann genau finden diese statt?

Die Übung EU PACE 17 baut auf der Übung EU CYBRID 17 auf. Die erste Durchführungsphase von EU PACE 17 findet zwischen dem 28. September und 4. Oktober 2017 statt. In der zweiten Durchführungsphase von EU PACE vom 17. bis zum 11. Oktober 2017 beteiligen sich die EU-Institutionen auf Arbeitsebene an der parallel verlaufenden NATO-Übung CMX 17.

3. Mit welchen Abteilungen nehmen die Verteidigungsministerien der EU- und NATO-Mitgliedstaaten an den beiden Übungen teil, und welche Teile der Übungen finden gemeinsam statt?

Auf die Antwort zu den Fragen 1 und 2 wird verwiesen.

4. Welche „Bedrohungen“ werden für die beiden Übungen angenommen und inwiefern trifft es zu, dass diese in einer Umgebung regelmäßiger Cyberangriffe sowie zunehmender „Fake News“ stattfinden?

Im Rahmen der Übungen EU CYBRID 17 und EU PACE 17 soll die Krisenbewältigung im Kontext von kombinierten Cyber-/Hybridkampagnen gegen EU Militärstrukturen geübt werden. Die Übung EU CYBRID 2017 ist als eine strategische Planübung mit Cyberbezug, die Übung EU PACE 17 ist als eine mit der NATO koordinierte, parallele Krisenmanagementübung angelegt, deren Fokus auf Krisenmanagement und Reaktionsfähigkeit in einer Umgebung hybrider Bedrohungen liegt.

Die Übungsszenarien umfassen auch Cyberangriffe und „Fake News“.

5. Welche Szenarien werden (auch in Kombination) in „EU CYBRID 2017“ und „EU PACE17“ bzw. etwaigen Vorübungen durchgespielt (bitte so detailliert wie möglich schildern)?

In dem Szenario der EU CYBRID 2017 unterliegt ein EU Hauptquartier multiplen Cyberattacken.

In dem Szenario der EU PACE 17 unterliegen eine erhebliche Anzahl von EU Mitgliedstaaten Cyber-Angriffen unterschiedlicher Natur und Intensität. Gleichzeitig kommt es zu erhöhtem und gesteuertem Falschmeldungsaufkommen.

Beide Szenarien haben insbesondere zum Ziel, die grenzüberschreitende und ressortübergreifende Zusammenarbeit im Krisenmanagement in einem hybriden Umfeld zu üben.

a) Inwiefern sollen sich die Übungen bzw. etwaige Vorübungen auch mit einem Eingreifen oberhalb der Schwelle eines bewaffneten Angriffs befassen, und welche Haltung vertritt die Bundesregierung hierzu?

Die Vorabinformationen zur Planübung EU CYBRID 17 umfassen Cyberoperationen unterhalb der Schwelle des bewaffneten Angriffs. Lediglich zwei Übungsmomente umfassen Cyberoperationen bis zur Schwelle des bewaffneten Angriffs. Ob während der Übung ein Eingreifen oberhalb der Schwelle eines bewaffneten Angriffs thematisiert wird, ist der Bundesregierung nicht bekannt.

Zu EU PACE 17 liegen der Bundesregierung keine entsprechenden Informationen vor.

b) Welche Reaktionen (auch im Cyberraum) sollen auf einen solchen Angriff durchgespielt werden (bitte möglichst die simulierten Angriffe und Gegenangriffe schildern)?

Ziel von EU CYBRID 17 und EU PACE 17 ist die Einübung der Anwendung bestehender Krisenreaktionsmechanismen der EU und der Mitgliedstaaten auf ein hybrides Szenario mit einem Cyber-Anteil.

Welche konkreten Reaktionen beübt werden, wird sich aus dem dynamisch angelegten Übungsverlauf ergeben.

c) Sofern die Bundesregierung zu den Szenarien noch keine Informationen erhalten hat, wann sollen diese vorliegen?

Auf die Antwort zu Frage 5 wird verwiesen.

6. Wann sollen welche „Injektionen" (etwa zur Eskalation der geübten „Krisen" und „Bedrohungen") im Rahmen von „EU CYBRID 2017" und „EU PACE17" erfolgen?

Die Übungen werden sich während der gesamten Übungslaufzeit dynamisch entwickeln.

7. Inwiefern sollen auch die Verteidigungsminister selbst an „EU CYBRID 2017" oder „EU PACE17" beteiligt werden, und nach welchem Verfahren sollen diese auf die Szenarien reagieren?

Auf die Antwort zu den Fragen 1 und 2 wird verwiesen.

8. Welche Aufgaben werden das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), die „EU Hybrid Fusion Cell" sowie das Kommunikationszentrum „EU STRATCOM EAST" im Rahmen der Übungen übernehmen?

Die Arbeitseinheit des EAD für Strategische Kommunikation ist für die Öffentlichkeitsarbeit für die Übung EU PACE 17 zuständig. Welche Rolle die EU STRATCOM EAST dabei spielen wird, ist der Bundesregierung nicht bekannt. Eine Beteiligung des Cooperative Cyber Defence Centre of Excellence und der EU Hybrid Fusion Cell ist nicht geplant.

9. Welche „Injektionen" (etwa zur Eskalation der geübten „Krisen" und „Bedrohungen") wird die NATO im Rahmen der Übungen „EU CYBRID 2017" und „EU PACE17" vornehmen, und inwiefern stehen diese im Kontext der NATO-Übung „NATO CMX 17"?

Die zweite Durchführungsphase der Übung EU PACE 17 und die NATO-Übung CMX 17 finden zeitgleich als koordinierte Übungen in Umsetzung der gemeinsamen NATO-EU-Erklärung vom Juli 2016 statt. Die Einspielung von Ereignissen im Kontext der NATO-Übung CMX 17 in die Übung EU PACE 17 ist grundsätzlich vorgesehen.

10. Wann beginnt und endet die Übung „NATO CMX 17", und wer nimmt daran teil?

Die Übung findet vom 4. bis 11. Oktober 2017 statt. Geplante Teilnehmer sind die NATO-Mitgliedstaaten, die Gremien und Stäbe der NATO sowie die Partnernationen Finnland und Schweden.

11. Welche Szenarien hat das NATO-CCDCoE nach Kenntnis der Bundesregierung auf der jüngsten Cyberübung „Locked Shields" durchgespielt (bitte möglichst die simulierten Angriffe und Gegenangriffe schildern)?

Bei der NATO-Cyber-Abwehr-Übung „Locked Shields 2017" haben alle technischen Angriffs- und Verteidigungsmaßnahmen ausschließlich in einer virtuellen Umgebung stattgefunden.

In der Übung wurde der Angriff auf einen Militärflughafen inklusive der Energieversorgung und zentraler Netzwerkkomponenten simuliert. Folgende Szenarien wurden durchgespielt:

- 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.

Durch eigenständige sog. Legal Teams wurden einzelne Szenare auch unter rechtlichen Aspekten bewertet und mögliche Handlungsoptionen aufgezeigt.

Die realitätsnahe Übungsannahme war, dass die Angreifer bereits Wochen zuvor die Systeme durch verschiedene Angriffe, wie z. B. Phishing-Mails, Innentäter oder Ausnutzung technischer Schwachstellen, mit Schadsoftware infiziert hatten.

12. Welche weiteren Cyberübungen sind auf Ebene der NATO und der Europäischen Union nach Kenntnis der Bundesregierung in Planung?

Die NATO-Übung CYBER COALITION wird vom 27. November bis zum 1. Dezember 2017 in Tartu, Estland, stattfinden. 2018 plant die EU die Übung CYPER EUROPE 2018 einschließlich der Vorübung EuroSOPEX.

13. Welche weiteren Anstrengungen unternehmen die Europäische Union und die NATO nach Kenntnis der Bundesregierung 2017 hinsichtlich gemeinsamer Trainings oder der Durchführung von Cyberoperationen?

Auf die Antwort zu Frage 12 wird verwiesen.

14. Was ist der Bundesregierung über den Stand der Einrichtung eines „Zentrums gegen hybride Bedrohungen“ („Hybrid-Kompetenzzentrum“) in Helsinki bekannt, wer arbeitet dort mit, und welche Aufgaben werden dort übernommen?

Das von Finnland gegründete Europäische Zentrum zur Bewältigung hybrider Bedrohungen befindet sich noch im Aufbau.

Es ist eine multinationale Forschungseinrichtung zur strategischen Analyse hybrider Bedrohungen, welche von Finnland zusammen mit Frankreich, Deutschland, Lettland, Litauen, Polen, Schweden, Großbritannien, Estland, Spanien sowie den USA und Norwegen aufgebaut wird.

15. Inwieweit liegen der Bundesregierung mittlerweile neuere belastbare Erkenntnisse zur Urheberschaft des Angriffswerkzeugs „Stuxnet“ vor, den sie als „Cyber-Sabotage auf Kritische Infrastrukturen“ bezeichnet, und mit welchem Ergebnis sind die vorliegenden Erkenntnisse durch das Bundesamt für Verfassungsschutz „hinsichtlich einer möglichen nachrichtendienstlichen Urheberschaft bewertet worden“ (Bundestagsdrucksache 18/164, Frage 42)?

Dem Bundesamt für Verfassungsschutz liegen keine neuen belastbaren Erkenntnisse zur Urheberschaft der Schadsoftware ‚Stuxnet‘ vor, die über die auf Bundestagsdrucksache 18/164 dargelegte Einschätzung hinausgingen.

16. Was ist der Bundesregierung über Planungen der US-Übung „Cyber Storm 2018“ des Heimatschutzministeriums bekannt, und inwiefern erwägt sie wieder eine Teilnahme (Bundestagsdrucksache 18/4286)?

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist bekannt, dass das Heimatschutzministerium mit den Planungen begonnen hat. Eine BSI-Teilnahme bei der „Cyber Storm 2018“ ist im Rahmen des International Watch and Warning Network vorgesehen.

17. An welchen Übungen oder Trainings hat das Bundeswehrkommando „Computer-Netzwerk-Operationen“ (CNO) seit seiner Gründung teilgenommen (Bundestagsdrucksache 18/4286, Frage 1)?

Die Antwort ist als Verschlusssache „VS – Nur für den Dienstgebrauch“ eingestuft und wird als Anlage übermittelt, da Angaben zu Übungen des Kommandos Computer-Netzwerk-Operationen (Kdo CNO) Aufschluss über Fähigkeiten des Kommandos geben könnten und damit die Sicherheitsinteressen der Bundesrepublik Deutschland betreffen.*

18. Inwiefern hat das CNO in der Vergangenheit auch geübt, „in gegnerische Netzwerke einzudringen, dort aufzuklären, einzelne Funktionen zu stören und zeitweise außer Betrieb zu setzen oder dauerhaft zu schädigen“ (Bundestagsdrucksache 18/4286, Frage 13)?

Das Kdo CNO hat in der Vergangenheit keine Übungen im Sinne der Fragestellung durchgeführt.

19. Wie oft ist das deutsche „Netzwerk gegen hybride Bedrohungen“ seit der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11543 (Frage 22) bereits zusammengekommen, und welche Themen standen dabei auf der Tagesordnung?

a) Welche einzelnen Arbeiten werden im Netzwerk von den Bundesministerien, dem Bundeskanzleramt, der Beauftragten der Bundesregierung für Kultur und Medien sowie dem Bundespresseamt übernommen?

b) Inwiefern wurden im Netzwerk auch Leitungs-oder Sekretariatsaufgaben vergeben, und von wem werden diese übernommen?

Die Beantwortung der Fragen 19a und 19b erfolgt gemeinsam.

Die Antwort der Bundesregierung auf Bundestagsdrucksache 18/11543 gilt unverändert. Seither gibt es weder einen neuen Stand noch haben weitere Sitzungen stattgefunden.

20. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat, bzw. liegen ihr hierzu nach wie vor keine Informationen darüber vor, dass es eine derartige, nicht von Staaten ausgeübte versuchte oder erfolgreich ausgeführte Attacke jemals gegeben hat (Bundestagsdrucksachen 17/7578, 18/164, 18/10759)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

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

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